

# **NAVAL POSTGRADUATE SCHOOL**

## **Monterey, California**



## **THESIS**

**DEVELOPMENT OF AN INFORMATION SECURITY  
AWARENESS TRAINING PROGRAM FOR THE ROYAL  
SAUDI NAVAL FORCES (RSNF)**

by

Sami M. Alageel

June 2003

Thesis Advisor:  
Second Reader:

J. D. Fulp  
Brian D. Steckler

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> June 2003	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Development of an Information Security Awareness Training Program for the Royal Saudi Naval Forces (RSNF)			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Sami M. Alageel				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b>  The Royal Saudi Naval Forces (RSNF) are vulnerable to the same kinds of threats to its information infrastructure as the rest of the industrialized nations. As an officer in the RSNF, I am familiar with the special information assurance needs and interests of my organization, and thus, I am in a position to leverage my formal Information Technology Management (ITM) education to address these needs. The United States has played a prominent lead role in establishing many educational curriculums in the area of information assurance (IA). Though the breadth and depth of educational curriculum and resource materials (i.e., universities, certification programs, computer-based training, Web content, etc.) is impressive; the sheer volume can be overwhelming and intimidating to the novice. What is needed is a methodical survey of the main IA themes that are currently emphasized by the most prominent and respected institutions offering IA training and education. This survey needs to be cross-referenced to identify core areas, and any other didactic information (e.g., models, rules, best practices, etc.) that might prove useful in developing the final training product for the RSNF.				
<b>14. SUBJECT TERMS</b> Awareness, Training, information technology, Information Assurance, Policy			<b>15. NUMBER OF PAGES</b> 102	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release: distribution is unlimited**

**DEVELOPMENT OF AN INFORMATION SECURITY AWARENESS  
TRAINING PROGRAM FOR THE ROYAL SAUDI NAVAL FORCES (RSNF)**

Sami M. Alageel  
Lieutenant, Royal Saudi Naval Forces  
B.S., King Fahad Naval Academy, 1991

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY  
MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2003**

Author: Sami M. Alageel

Approved by: J. D. Fulp  
Thesis Advisor

Brian D. Steckler  
Second Reader

Dan Boger  
Chairman, Department of Information Systems

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

The Royal Saudi Naval Forces (RSNF) are vulnerable to the same kinds of threats to its information infrastructure as the rest of the industrialized nations. As an officer in the RSNF, I am familiar with the special information assurance needs and interests of my organization, and thus, I am in a position to leverage my formal Information Technology Management (ITM) education to address these needs. The United States has played a prominent lead role in establishing many educational curriculums in the area of information assurance (IA). Though the breadth and depth of educational curriculum and resource materials (i.e., universities, certification programs, computer-based training, Web content, etc.) is impressive; the sheer volume can be overwhelming and intimidating to the novice.

What is needed is a methodical survey of the main IA themes that are currently emphasized by the most prominent and respected institutions offering IA training and education. This survey needs to be cross-referenced to identify core areas, and any other didactic information (e.g., models, rules, best practices, etc.) that might prove useful in developing final training products for the RSNF.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>II.</b>	<b>COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS.....</b>	<b>3</b>
<b>A.</b>	<b>WHAT EVERYONE NEEDS TO KNOW .....</b>	<b>3</b>
<b>1.</b>	<b>What Resources Are We Trying to Protect.....</b>	<b>4</b>
<b>a.</b>	<b><i>Information</i> .....</b>	<b>4</b>
<b>b.</b>	<b><i>Services</i>.....</b>	<b>5</b>
<b>c.</b>	<b><i>Equipment</i> .....</b>	<b>5</b>
<b>2.</b>	<b>Against What.....</b>	<b>5</b>
<b>a.</b>	<b><i>Malicious Threats</i> .....</b>	<b>6</b>
<b>b.</b>	<b><i>Unintentional Threats</i>.....</b>	<b>7</b>
<b>c.</b>	<b><i>Physical Threats</i>.....</b>	<b>7</b>
<b>B.</b>	<b>WHY IS ISATP IMPORTANT FOR THE RSNF .....</b>	<b>7</b>
<b>C.</b>	<b>WHO SHOULD ATTEND ISATP .....</b>	<b>8</b>
<b>III.</b>	<b>THE SUGGESTED AWARENESS TRAINING PROGRAM.....</b>	<b>11</b>
<b>A.</b>	<b>ANALYSIS OF VARIOUS EXISTING TRAINING PROGRAMS .....</b>	<b>11</b>
<b>1.</b>	<b>SANS Institute.....</b>	<b>12</b>
<b>2.</b>	<b>Naval Postgraduate School (NPS) .....</b>	<b>14</b>
<b>3.</b>	<b>Learning Tree International .....</b>	<b>15</b>
<b>4.</b>	<b>Laptop Training Solutions .....</b>	<b>16</b>
<b>B.</b>	<b>NEEDS ASSESSMENT.....</b>	<b>17</b>
<b>C.</b>	<b>AWARENESS TRAINING STRATEGY AND PLAN .....</b>	<b>18</b>
<b>•</b>	<b>Length and quality.....</b>	<b>18</b>
<b>•</b>	<b>State-of-the-art Material .....</b>	<b>19</b>
<b>•</b>	<b>Trainees' availability .....</b>	<b>19</b>
<b>D.</b>	<b>ESTABLISHING PRIORITIES.....</b>	<b>20</b>
<b>E.</b>	<b>MATERIAL COMPLEXITY .....</b>	<b>21</b>
<b>F.</b>	<b>SELECTING AWARENESS TRAINING TOPICS .....</b>	<b>22</b>
<b>IV.</b>	<b>THE AWARENESS TRAINING PROGRAM AND IT'S IMPLEMENTATION .....</b>	<b>25</b>
<b>A.</b>	<b>PROPOSED AWARENESS TRAINING MATERIAL .....</b>	<b>25</b>
<b>B.</b>	<b>TECHNIQUES FOR DELIVERING THE AWARENESS TRAINING MATERIAL .....</b>	<b>53</b>
<b>C.</b>	<b>EVALUATION AND FEEDBACK .....</b>	<b>55</b>
<b>D.</b>	<b>ONGOING IMPROVEMENT .....</b>	<b>56</b>
<b>V.</b>	<b>CONCLUSION AND RECOMMENDATION .....</b>	<b>57</b>
<b>A.</b>	<b>CONCLUSION .....</b>	<b>57</b>
<b>B.</b>	<b>RECOMMENDATIONS FOR FUTURE WORK.....</b>	<b>58</b>
<b>APPENDIX A</b>	<b>- SANS TRACK 1 COURSE OUTLINE.....</b>	<b>61</b>
<b>APPENDIX B</b>	<b>- NPS INFORMATION ASSURANCE (IA): COMPUTER SECURITY COURSE OUTLINE.....</b>	<b>65</b>

<b>APPENDIX C - LTI INTRODUCTION TO SYSTEM AND NETWORK SECURITY COURSE OUTLINE.....</b>	<b>69</b>
<b>APPENDIX D - LAPTOP SOLUTIONS COMPTIA SECURITY+™ CERTIFICATION EXAM TRAINING COURSE OUTLINE .....</b>	<b>71</b>
<b>APPENDIX E - PROPOSED ISATP MATERIAL OUTLINE.....</b>	<b>75</b>
<b>LIST OF REFERENCES.....</b>	<b>79</b>
<b>BIBLIOGRAPHY .....</b>	<b>83</b>
<b>INITIAL DISTRIBUTION LIST .....</b>	<b>85</b>

## LIST OF FIGURES

Figure 1.	Different Areas of Security Threats.....	6
Figure 2.	ISATP Management.....	20

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Training Delivery Techniques. From Ref. [30].....	55
Table 2.	Terminologies and Core Concepts Covered by SANS Security Essential Course Topics. [4].....	64
Table 3.	Information Assurance (IA): Computer Security Course. (From: [6]).....	67
Table 4.	Learning Tree International- Introduction to System and Network Security Course.[7].....	70
Table 5.	Laptop Solutions CompTIA Security+™ Certification Exam Training Course.[8].....	74

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

This thesis owes its existence to the help, support, and inspiration of many people. In the first place, I would like to express my sincere appreciation and gratitude to Professor. John D. Fulp of the NPS Computer Science Department for his support, guidance, and encouragement and excellent advice throughout this thesis. I would also like to express my acknowledgment and gratitude to Professor Brian Steckler for his guidance and direction. Finally, I would like to express my deepest gratitude for the constant support, understanding, love, sacrifice and patience that I received from my wife, my children, Saud, Reema and my parents during the past two years in the USA.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION**

Rapid advances in Information and Communication Technology have a profound effect on our Navy. Information is becoming the most important factor. Militaries in general are becoming increasingly dependent on computer technology for every facet of their operations in today's information technology environment. Information security is critical to the success of the RSNF, and achieving this security is greatly dependent on each user's awareness and behavior along with a thorough understanding of the risks to which our information assets may be subjected. This awareness is a necessary starting point for the development of a successful information security training program. The constant development and deployment of new viruses and worms, the abundance of Internet attacks, and the occasional system abuse by authorized users, all require the user to be knowledgeable and attentive. In the RSNF, computer systems and resources are used every day to complete mission critical tasks. Thus, it is important for us to understand the risks of allowing end users who are not aware of computer security considerations to operate these systems, resulting in potential exploitation by our enemies. The critical role that awareness plays in this environment has been championed extensively in Information Assurance literature. This excerpt from Native Intelligence Inc website is representative of such sentiment:

Security apathy and ignorance are the biggest threats to computer systems. . . . And the best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem -- it's by raising awareness training and educating all computer users in the basics of computer security.

With the growth of the Internet and the potential increase of utilizing Internet technologies inside the RSNF, more and more computing resources have become connected to networks that can potentially be reached from both outside and inside the Navy's system infrastructure perimeter. Simply stated, as connectivity increases, the risk of attack on our networks increases. When we are dealing with information security specifically, though, there are three issues influencing the need for an Information Security Awareness Training Program that stand out for their clear agreement: confidentiality, integrity, and availability (CIA). Information can reasonably be called

secure when these three properties are present. In theory, the goal of this Information Security Awareness Training Program is straightforward. The goal is to minimize the risk associated with the use of the Navy's systems and computers by addressing the two constituent components of risk: threats and vulnerabilities, this training program will focus on the "safeguards" component of risk reduction; specifically, their selection and employment to protect the confidentiality, integrity and/or availability of the Navy's systems. Addressing the risks, threats and vulnerabilities, and applying the safeguards learned from this course will leave us with the portion of risk remaining after security measures have been applied or what is known as residual risk. The relationship between these three key elements can be represented in a formulated way as follows:

$$\text{Risk} = \text{Threats} \times \text{Vulnerability}$$

$$\text{Residual Risk} = \text{Risk} - \text{Safeguards}$$

$$\text{Therefore: Residual Risk} = (\text{Threats} \times \text{Vulnerabilities}) - \text{Safeguards}$$

This thesis will research various prominent computer security training programs that are already in existence, and will then suggest a composite program customized to meet the needs of the Royal Saudi Naval Forces. RSNF and the other branches of the Ministry of Defense and Aviation (MODA) cannot protect the confidentiality, integrity, and availability of information in today's highly networked system environment without ensuring that each person involved understands their responsibilities within the RSNF and is sufficiently trained to perform them.

Chapter II of this thesis will present an introduction to security awareness training programs, in general, and then continue to argue why such programs are important to the Saudi Navy. In the final section of Chapter II, I will identify the intended target audience of this course; i.e., who should be trained in computer security. In Chapter III, I will present the outcome of my analysis of the various existing programs, followed by my assessment of their application for the RSNF. Chapter III will also develop the awareness training plan and strategy then conclude with the awareness training topics selection criteria that will fit the needs of RSNF. Chapter IV will propose the awareness training material for the ISTAP and then cover the implementation plan for the proposed program along with how it will be delivered to the target audience. Chapter V will conclude this thesis and provide some recommendations for further research on this topic.

## **II. COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS**

This chapter provides an overview of the information security awareness and training programs, and answers the question of why such programs are important to the RSNF. This chapter also addresses who should be attending these programs in the Saudi Navy.

### **A. WHAT EVERYONE NEEDS TO KNOW**

There is an old saying that a chain is only as strong as its weakest link. While organizations around the world regularly employ the use of powerful firewalls, antivirus software and sophisticated intrusion-detection systems to safeguard valuable information assets, they often pay too little attention to the most important and vulnerable security component: the human part. In virtually every aspect of our lives that entails the operation of sophisticated technology, we have to be certified in some way or another. Whether we drive a car or repair an aircraft, we need some kind of knowledge-validating certificate, yet we are free to use computers and the various networks within the Navy without any sort of training and certification on the security aspects and potential risks associated with their use. When these assets are attacked, damaged or threatened, the confidentiality, integrity and availability (CIA) of our data and the proper operation of the RSNF may be interrupted.

The cause of interruptions can range from errors affecting information integrity to viruses destroying entire computer centers. Losses can vary, for example, from the actions of apparently trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer-related information losses is not possible because many losses are never discovered, and others are intentionally buried to avoid unfavorable publicity. The effects of various threats vary considerably, yet all effects can ultimately be classified into one or more of the three security attributes of information: confidentiality, integrity or availability.

The Royal Saudi Naval Force strives to make resources readily available to all employees, from commanders to data entry clerks, in a developmental environment where data sharing is essential for conducting daily businesses. Promoting a secure computing strategy may seem difficult. Computer networks present a new set of challenges to administrators and technical support personnel for providing a secure working environment. Today, information security is a much bigger issue and the context is difficult to define. The dangers are real with threats that multiply and divide. The threats come from both insiders and outsiders, feeding off vulnerabilities that are inherent in the technology and the users. It is intimidating for technical support personnel in the RSNF, who quite often have other professional responsibilities, to identify, quantify, and justify the measures necessary to maintain a safe and secure network installation. We can make tremendous progress toward achieving a more secure computing environment by drafting and enforcing a thorough security policy and educating our personnel to both understand and follow its mandates via an effective awareness training program.

Since security is everyone's responsibility, RSNF personnel need to know what threats they are facing and what they can do to diminish those threats. We have to make sure that everybody within the RSNF understands the value of their information assets and the tools that will help them protect it. We need to change the way we think and act, so that security is not an add-on, but rather an integral part of our daily use of all information systems and networks. What we need exactly is a move toward a 'culture of security'. [1, 3]

## **1. What Resources Are We Trying to Protect?**

A basic goal of Information Security Awareness Training Programs is to reduce vulnerabilities in our RSNF Information Infrastructure by promoting widespread education in computer security and to protect resources and assets from loss. Resources may include the following.

### ***a. Information***

Information systems have not been designed to be secure. The security that can be achieved through technical means is limited. Recently, there has been an

increase in the awareness for the need within government agencies to protect sensitive, proprietary and secret information. Proper understanding of the importance of information in our world, offers the following:

The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data. It's all just electrons.... There's a war out there ... and it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think, it's all about information [Cosmo from the Movie 'Sneakers'].

In many instances, what we are trying to protect is information. In today's "information age", information is vital and has a huge value. This value could be defined or it could be perceived. The fundamental principles of information security are confidentiality, availability and integrity. We must look at each of these principles and relate them to our training program objectives.

#### ***b. Services***

This includes systems and applications, because new exploits are written every day, and because not all of them involve viruses and buffer overflows, we should pay attention to the applications and whether their security patches are current or not.

#### ***c. Equipment***

Equipment includes computers and networking components, and in particular, computer consoles and sensitive network equipment such as routers, hubs and switches. One example is computer thefts. The loss of equipment can result in financial loss to the RSNF, but it can also have serious effects if the data lost with the equipment had not been backed up in a timely manner or was sensitive to disclosure.

## **2. Against What**

The growing complexity of security threats creates new issues for enterprise managers to deal with as they try to protect themselves. A threat is defined as "any circumstance or event with the potential to cause harm to an information system in the

form of destruction, disclosure, adverse modification of data, and/or denial of service [NSTISSI 4009]”. When facing the issue of security, it is important to understand exactly what are we trying to protect. Information is the RSNF’s and every organization’s most important asset and must be protected from unauthorized access. Figure 1 introduces a layout that can be used to divide security threats into different areas.



Figure 1. Different Areas of Security Threats.

#### **a. Malicious Threats**

Malicious threats usually come from non-employees (i.e., outsiders) or disgruntled employees (i.e., insiders) who have an adverse goal or objective to achieve, and are in a position to exploit one or more security vulnerabilities. Malicious attacks vary in their targets, methods, and motives but are usually covert acts by individuals who wish to harm the system or prevent others from using it. Hackers disrupt normal business operations by exploiting a business' vulnerabilities. They use various techniques, methods, and tools to accomplish this. We need to understand the various aspects of security to develop measures and policies to protect our assets and limit their vulnerabilities.

The correct term to use for someone who maliciously breaks into systems is “cracker.” Common methods for gaining access to a system include password cracking, exploiting known security weaknesses, network spoofing and social engineering.

Malicious attackers normally will have a specific goal, objective, or motive for an attack on a system. These goals could be to disrupt services and the continuity of business operations by using denial-of-service (DoS) attack tools. They might also want to steal information or even steal hardware such as laptop computers or Personal Digital Assistants (PDAs).

***b. Unintentional Threats***

Unintentional threats can range from a user who accidentally deletes important operating system files to loading unauthorized software that has a virus. Greater precautions must be taken for users with access to data that are more sensitive. An example of a non-malicious attack is when an employee copies games from a diskette onto a local hard drive and then runs the executables. If any of the games contain a virus or Trojan horse, and the organization has not yet deployed any anti-virus software, employees will begin to notice strange and unforeseen events occurring on their computers, causing disruption of services and possible corruption of data.

***c. Physical Threats***

Physical security, an integral part of protecting data, is vital in a balanced security program. Physical security involves protecting offices containing computers and related equipment from environmental threats (e.g., fire and flood), physical threats from people, and various other forms of equipment and environmental contamination. Physical security is one of the most important aspects of computer security. It is also one of the most often overlooked aspects. Physical security also deals with protecting our systems from intruders who use or attempt to gain physical access to the system to conduct exploitation via technical means (e.g., capturing password files or installing a login-capturing artifice).

**B. WHY IS ISATP IMPORTANT FOR THE RSNF**

Awareness and training plays an important role in achieving the RSNF goal of computer security. Providing periodic information security awareness training to

employees who are involved in the management, use, or operation of computer systems under their control is critical. The training objectives are to enhance employee awareness of the threats and vulnerabilities to their computer systems; and to promote the use of improved computer security practices within the Navy. The RSNF Information Security Awareness Training Program (ISATP) is a tool to educate RSNF personnel on their responsibility to protect the confidentiality, availability and integrity of information and information processing systems. We need to understand that information security is not just a technology concern. We should give equal attention to human management and the security behavior of employees, and we will strive to build a better information security awareness and training program throughout the RSNF that is based on the principles described later in this thesis.

Obviously, information security has to be improved upon if we are to properly protect the RSNF's valuable information assets. Until now, however, most of the focus on solving RSNF information security problems has been focused on technology. This approach has regrettably ignored one of the most important elements of successful information security: the human aspect. This Information Security Awareness Training tries to correct this discrepancy by directing more attention to what humans can do as individuals and as a team of employees to significantly improve information security in any organization. Information security professionals have long realized the need to inform, educate and manage the "human" side of information security. The idea that people are at the center of the problem of security breaches is common, but many organizations are still struggling with the following questions: "How do we deal with the human part? How do we tackle information security from a non-technical standpoint that can be appreciated by normal users and may increase our organization's overall security? Who needs to be trained and educated in information security"? This thesis will address these questions and propose answers to them.

### **C. WHO SHOULD ATTEND ISATP**

The human element poses the greatest risks to information security. Operating systems can be hardened, virus scans can be conducted on a regular basis, and hardware can be physically secured. However, if employees of the RSNF do not understand and

embrace basic information security best practices, the other security initiatives have no meaning. This course is designed for all RSNF personnel, from Executive Leadership, section leaders, and ship commanders, to the soldiers and clerks entering data into databases.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. THE SUGGESTED AWARENESS TRAINING PROGRAM**

Now that the need for an Information Security Awareness Training Program (ISATP) for the Royal Saudi Naval Forces has been established, the next logical step is to define the scope and essential elements of such a program. The first part of this chapter will analyze selected information security awareness training courses offered by four dominant and respected information assurance (IA) curriculum providers. The guidelines developed in this thesis define a minimum set of expectations. The guidelines will be reviewed as necessary to reflect future changes in the use of technology, RSNF and Government Laws and Policies. The analysis of these courses will help in identifying appropriate information security awareness training material that will aid in achieving and maintaining enhanced levels of confidentiality, integrity and availability for specified information within the RSNF.

The second part of this chapter will discuss the RSNF awareness training needs assessment. The result of this assessment will rationalize the selection of the terminology and core concepts that will be included in the ISATP, and to persuade the managers in RSNF to allocate adequate resources to meet those needs. The third part of this chapter will present the security awareness training strategy and plan. The plan will define the strategy of developing and implementing the ISATP in the Royal Saudi Naval Forces.

The fourth part of this chapter will discuss and establish priorities regarding who needs to be trained, when the training should be delivered, and what should be considered when prioritizing the training. The fifth part of this chapter will answer the question of how detailed this program will be and why? The last part of this chapter will justify the reasons why these awareness topics were selected. This justification will be derived from the analysis of the four courses and from the needs assessment of the RSNF.

#### **A. ANALYSIS OF VARIOUS EXISTING TRAINING PROGRAMS**

The majority of IA professionals agrees that security awareness training is critical to managing enterprise risk, yet most information security practitioners say their training programs are inconsistent at best -- and ineffective at worst. Security awareness training

has always been difficult to execute. However, with the wide availability of awareness training courses offered by commercial, educational, and governmental organizations these days, the tools to engineer a meaningful ISATP are available.

I have selected four basic information security courses to be analyzed in this thesis. These four courses are offered by four distinct security training providers. The analysis will include a historical background of these providers and their experience in the field. It will also include the terminologies and core concepts covered by each. These providers and detailed information of the topics covered by their courses are discussed below.

## **1. SANS Institute**

The first provider discussed is the SANS Institute. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. [4]

Many SANS resources, such as news digests, research summaries, security alerts and papers are free. Income from printed publications funds university-based research programs. Income from SANS educational programs fund special research projects and SANS Training programs. The SANS community supports various programs and products including:

- Information Security Training
- The Global Information Assurance Certification (GIAC) Program
- SANS Resources
- Internet Storm Center
- Center for Internet Security and Security Consensus Operational Readiness Evaluation (SCORE)
- SANS/FBI Top Twenty List

SANS training provides a core set of educational courses designed to help master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited. The courses were developed through the community consensus of hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and the in-depth technical aspects of the most crucial areas of information security. SANS training is provided in a classroom setting from SANS-certified instructors, or can be self-paced over the Internet. SANS programs have educated many thousands of security, networking, and system administration professionals in the world. [4]

SANS also offers a Volunteer Program through which, in return for acting as an important extension of the SANS conference staff, volunteers may attend classes at no cost. Volunteers are most definitely expected to pull their weight and the educational rewards for doing so are substantial. SANS Track 1: Security Essentials, enables novice students to learn the full SANS Security Essentials curriculum needed to qualify for the GIAC Security Essential Certification (GSEC), which is one of a series of Global Information Assurance Certification (GIAC). [4]

In this track, students will learn the language and underlying theory of computer security, and at the same time, will learn the essential, up-to-the-minute knowledge and skills required for effective performance. This course meets both of the key promises SANS makes to their students: (1) they will gain up-to-the-minute knowledge they can put into practice immediately upon returning to work; and (2) SANS identifies the best security instructors to teach their courses, by choosing from those who have ranked highest in a nine-year competition among potential security faculty. This program offers great teaching along with the ability to master the material needed for the two most popular certifications in information security: Certified Information Systems Security Professional (CISSP) and GIAC Security Essentials Certification (GSEC). Appendix A has a fully detailed table of terminologies and core concepts covered in this six-day course. [4]

## **2. Naval Postgraduate School (NPS)**

The second provider is the Naval Postgraduate School's Center for Information Systems Security (INFOSEC) Studies and Research (NPS CISR). NPS has been home to a vibrant program in computer and network security since 1990. Located in Monterey, California, CISR was one of the first efforts of its kind to develop a program of tightly coupled research and instruction on IA topics at the graduate level. For over a decade, CISR's program of classes, research, visiting professors, workshops, academic outreach, short courses in IA, and invited lecture series have set the standard of excellence in computer information security research. Each year over 400 military and civilian NPS students use the CISR laboratories for coursework and research, and CISR supports more graduate student thesis research in IA than any other program in the United States. [5]

Designated by the National Security Agency (NSA) as a National Center of Excellence in IA education on April 14, 2000, the Naval Inspector General noted in his Command Assessment of NPS that CISR "has developed an outstanding and comprehensive IA curriculum. Undoubtedly, CISR's immediate return on investment for the services is the cutting-edge knowledge and experience our graduates apply to current operational assignments". [5]

The CISR philosophy is based on the fact that classes and research examine the problem of malicious software and system subversion. Using foundational concepts and technologies as a springboard for new developments, students and faculty construct systems to provide high confidence of enforcement for critical security policies in the face of all malicious software and penetration attempts, including those that are not yet known. They believe security and assurance should be built into systems from the start rather than as an afterthought or as a series of continuing updates and patches. To that end, CISR involves synergistically related classes, laboratory work and research of faculty, students and staff, making CISR truly a valuable DoD resource for leading edge IA research and education. [5]

The NPS CISR is the world's foremost center for military research and education in Information Assurance (IA), defensive information warfare, and computer and network security. CISR's mix of experienced military officers and government and civilian

students make it uniquely qualified to address security issues of the Department of Defense (DoD) and U.S. Government. CISR is also known throughout the field as one of the most innovative security research groups in the world and is unsurpassed in producing a cadre of military officers with Master's or Ph.D. degrees qualified for assignment to critical IA-related roles. Their graduates have state-of-the-art systems security and IA knowledge and an advanced degree in Information Sciences. [5]

In particular, I will analyze their CS-3600 (Introduction to Computer Security) Course. This 12 week course is concerned with fundamental principles of computer and communications security for modern monolithic and distributed systems. It covers privacy concerns, data secrecy and integrity issues, as well as U.S. DoD security policy. Security mechanisms introduced will include access mediation, cryptography, authentication protocols, and multilevel secure systems. Students are introduced to a broad range of security concerns including both environmental as well as computational security. Laboratory facilities are used to introduce students to a variety of security-related technologies including, discretionary and mandatory access controls (DAC and MAC) in both low and high assurance systems, identification and authentication protocols, the use of cryptography in distributed systems, classes of malicious software, and basic network filtering technology (firewall operation). [5]

Appendix B lists the main terminologies and core concepts covered in the topics of this course.

### **3. Learning Tree International**

Learning Tree International is a world leader in hands-on training for IT Professionals. Over 1.3 million course participants from more than 18,000 companies have attended their IT courses led by expert instructors with real-world experience. Courses are presented at Learning Tree Education Centers and other locations throughout the world, as well as on-site at client facilities. They offer over 150 courses in today's hottest technologies, including Windows XP, 2000, .NET, Java, XML, Oracle9i and 8i, UNIX and IT Management, information security along with 42 Professional Certification Programs. [7]

They state that each of their intensive 4 and 5-Day hands-on courses are designed to help attendees acquire the skills they need...fast and in-depth. Since their training is job role-focused, attendees are able to apply their new skills the day they return to work and begin reaping the benefits immediately. Learning Tree Course instructors work full time in high-tech companies, R & D labs and other business environments where they use the very technologies they teach, since they have already solved the same technical problems we are likely to encounter. They say that they have a unique Multimedia Display System used in their Education Center courses, and that with their state-of-the-art, proprietary display system, the instructor will annotate and manipulate information in real time on two independent projection screens. According to the Learning Tree website, this powerful teaching tool will give their instructors greater flexibility to customize and pace the course presentation. [7]

Learning Tree presents over 8,000 course events annually at their Education Centers in Washington, D.C., New York City, Atlanta, Boston, Chicago, Los Angeles, Ottawa, Toronto, London, Paris, Stockholm and Tokyo. The courses are also available for presentation on site at workplaces. A full list of topics and core concepts covered in their (Introduction to System and Network Security) course are listed in appendix C.

#### **4. Laptop Training Solutions**

Students in their Laptop Training Solutions, will receive a laptop computer with OMNI award winning LBT, which includes the best instructional design and graphic learning systems, state-of-the-art simulations and exam preparation software to create an unparalleled learning experience. Also included is a set of authorized study manuals for selected courses of study. You have the convenience of studying at your home or in an environment of your choosing, and when your schedule allows. You can then frequent the state of the art networking labs, or set up your own lab at home. Laptop Training Solutions' revolutionary training products use "applied simulation" to give students experience with courses of study. Certified professional guided study groups are available in the daytime, evenings and on weekends, which provide direction and answers to questions. Support is also available through e-mail, telephone, and on-line support through student services. [8]

The CompTIA Security+™ vendor-neutral certification exam is the worldwide standard of competency for foundation-level security practitioners. The demand for skilled security professionals is growing significantly. The technology community identifies Security+™ as the perfect way to validate your knowledge of information security. The Laptop Training Solutions will prepare students for this exam by providing them with study manuals, computer and exam preparation software simulations. Appendix d has a list of the topics and core concepts covered in these learning resources.

## **B. NEEDS ASSESSMENT**

Security awareness and training should be focused on the RSNF's entire employee population. Executives must set the model for proper INFOSEC conduct within the Navy. An awareness training program must begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. This course will be developed specifically to train and help Royal Saudi Naval Force employees understand the vulnerabilities of the automated information systems that support the RSNF infrastructure. In addition, this course will assist these employees in minimizing the risk associated with their use of these systems. An important result of supplying such baseline standards of INFOSEC is nurturing a commitment to improve RSNF's attitude toward information security.

Employees exposed to computers and information systems will be trained in information security, so they can use their technical skills along with the knowledge obtained from the ISATP course to promote a more secure RSNF IT environment. The ISATP course is a baseline course outline. The final results of this course are highly dependent on the INFOSEC topics and concepts included in its syllabus. I conducted this study of trends identified in industry, academic, or U.S. government publications and by information security training organizations. The use of these well-known and professional courses provides me with an insight into what should be taught in the RSNF ISATP. Furthermore, my 10 years of experience in Information Systems in the Saudi Navy, and the review and assessment of the available resource materials and courses, provided me with the solutions for the awareness training needs of the RSNF, And the gaps between the level of information security we need in RSNF and what is being done.

The ISATP should be designed to provide its participants with core IA knowledge and practical techniques for protecting the security of RSNF information infrastructure. Security issues, technologies, and recommended practices should be addressed at increasing layers of complexity, beginning with concepts and proceeding on to technical implementations. The principles, strategies, and practices covered must be applicable to most system platforms and network environments in the RSNF.

### **C. AWARENESS TRAINING STRATEGY AND PLAN**

Awareness training strategy pertains to the training team's understanding of the priority needs and how complex the recommended materials are. This information is based on an assessment of the audience, the working environment, the end goals desired, and availability of trainees. After identifying the core information security training topics from the analysis of the four existing courses described in section A of this chapter, we need to develop a strategy for implementing the resulting ISATP. While the possible elements of a successful awareness training strategy are limitless, here are some of the most common ones.

- **Length and quality**

Length and quality of training are the most obvious strategic elements. These two elements are generally in opposition to one another. The strategy may be either one of: a) very high quality/depth, but of excessive length, or b) of shorter duration, but lacking sufficient quality/depth. I endeavor to establish the ideal length versus quality tradeoff by scoping the ISATP material to only that which is deemed critical at the user awareness level, vice what is more appropriately addressed by systems designers and engineers. I rely largely on my personal experience and education in determining where that virtual boundary lies.

- **State-of-the-art Material**

Offering the most technically advanced awareness training material can form a powerful awareness training strategy. In the RSNF we need to have the capability to offer state-of-the-art training by training the trainers and keeping them updated in the IA field.

- **Trainees' availability**

Organizations realize significant savings on training and associated travel costs if we can offer the employees training without them having to leave their sites. This can be achieved by providing the training using either a web-based model, CD's, or having a mobile training team. In this way, training is no longer limited by physical location, but is instead based only upon the trainees' availability.

What is important now is to define the roles of the Information and Computer Department and the responsibilities, of the Training and Security Departments in the Navy in regards to who, where, when and how this course will be presented and taught within the Navy.

The idea of the implementation of ISATP in the RSNF in this thesis will be based on the assumption that this course will be designed, developed and maintained by the Information and Computer Department in the RSNF HQ, which will be considered as the central security awareness training authority in the RSNF. The Information and Computer Department should establish and disseminate a security policy and then assign the responsibility for enforcing this policy to the organizational units. The Information and Computer Department should also design, develop and maintain the information security awareness training program (ISATP) material and provide it to the training department for execution and implementation.

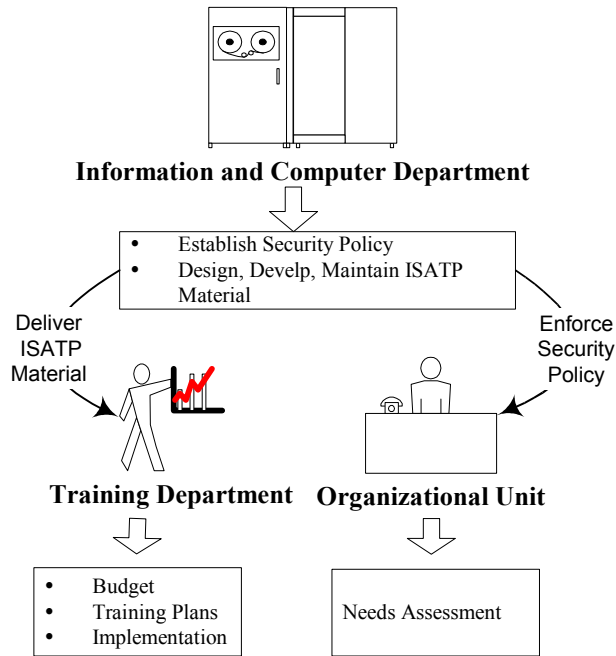


Figure 2. ISATP Management.

Prior to delivery of the training, a pilot group should be used to test training procedures and materials. This pilot will be a control group, ideally located at RSNF headquarters, which will allow the training team to have better communication and quick feedback from the pilot group. The pilot training session should be conducted by the Information and Computer Department within a specific timeframe to obtain feedback and make necessary changes before delivering the course to the training department.

#### D. ESTABLISHING PRIORITIES

Prevention is certainly better than cure, and securing computer systems is one of the best examples of this. Computers and networks are large, complex systems, so the best we can achieve is to reduce the likelihood of a break-in. It is never realistic to expect a completely secure system environment, especially if it is connected to a network. To successfully meet a training task, especially with limited resources, equipment and personnel, we must establish priorities. Establishing priorities helps promote an effective and efficient training program in the RSNF, and improve education and the level of awareness of the trainees. These priorities will address who should be trained first along with the subject matter they should receive. The program is open to all personnel without

restrictions; however, employees in security, intelligence, the information and computer department, human resources and command and control center members are especially encouraged to attend ISATP. In my opinion, the training in information security should start at the top of the organization, as educating managers in information security will sell them on the merits of such education, and hence, will encourage them to have their employees enrolled in the program. There are some key jobs, which I recommend we start with, and these include:

- Managers and Security Officers
- Communication and IT Specialists
- Systems Administrators
- Web Administrators
- Network Engineers

The training team will base the level of course detail on who is attending the course and how much time is available. Executives and top managers will have less time available than clerks and data entry personnel, for example.

## **E. MATERIAL COMPLEXITY**

The practice of training and keeping end-users updated with regards to information security does not have to be complicated. Many organizations accomplish this with a moderate budget and moderate levels of complexity. Practicing the implementation of ISATP in the RSNF does not mean that all end-users need to be certified in security. What we need simply is to make the end-users aware of security. Users need to understand that security is a very serious matter, and that the only way to keep the RSNF secure is to have everyone be responsible for his own part. Some important concepts that ISATP should stress to the end-users include:

- Good software installation practices: employees must know when it is not proper to install or run an application (e.g., from e-mail attachments, from unknown/untrusted web sources, or from an un-scanned floppy disk, etc). It is great if a policy exists that controls this issue, but it is necessary to ensure that the end-users know why this is important or they will never follow it
- Good awareness practices: End-users should be aware of activities concerning or affecting them and their systems. They need to know that

they are likely to be a witness to a hacker's activity more than an administrator.

- Good web-browsing practices: End users should know which sites not to access, what information is or is not safe to provide over the web, and they should understand basic browser security terminology and practices.
- Good confidentiality practices: It is important that everyone knows what is confidential and not confidential within the RSNF, both in general, and in their specific working environment .[10]
- Good system security practices: End users must know the critical role of passwords, regular data backups, uninterruptible power supplies, firewall protection, need ensure that the system is configured with the latest service packs, device drivers, application compatibility updates, and system security updates as soon as they're available.

No matter how complex the ISATP materials are, total security can never be achieved. Care should be taken not to select materials just because they are available. For example, there are probably several hundred Information Assurance (IA) courses available on the market, but few of them are suitable for the RSNF. The purpose of this course is not to present the latest security threats and protection technologies, but rather to introduce RSNF employees to the more common, everyday security practices that will best meet the information assurance needs of the RSNF.

## **F. SELECTING AWARENESS TRAINING TOPICS**

Selecting awareness training topics that meet RSNF needs is the main objective of this thesis, and the most difficult part. It is difficult because ISATP is just a start and the fact that this training program will be attended by the vast majority of the RSNF employees regardless of their position in the hierarchy of the Navy. Furthermore, the ISATP should reflect the security policy of the Navy. It may seem difficult for a single program to satisfy all types of employee needs within the RSNF, and indeed, for this reason, the course will be generic, avoid technical complications, and focus on the fundamentals and on building a precise vocabulary of IA terms and concepts. When determining the topics best suited to include in the ISATP, the following should be taken into consideration:

- Information relevance: Is the information provided appropriate to the audience level, well organized and easy to use?

- Information sources: Does the information come from primary resources (i.e., textual material, abstracts, and web pages)?
- Training material: Can it be developed within the proposed budget? What are the constraining factors for producing this material? Will the technology likely change before the proposed training material can be produced?
- Time: What are the critical time factors involved? When and how many learners must be trained within a given time frame? Is there more than one group to be trained?
- Instructors: Are they qualified for these types of courses? Do we have to train the instructors and bring them up to speed? How long will it take to bring them up to speed? How many instructors are available for this course?
- Self-Teaching Package: Are books and materials available? Are they geared to the student's educational level? Are the employees motivated to learn on their own?[10]

Training material and topics selected in ISATP will provide the skills necessary for RSNF employees to accomplish the security responsibilities associated with their job. The selection of the awareness training topics will be based on the common concepts covered by the four programs analyzed earlier in this chapter. This course will be reviewed, changed and modified frequently based on the changing needs of the RSNF as new threats, vulnerabilities and safeguards are discovered or introduced.

THIS PAGE INTENTIONALLY LEFT BLANK

## **IV. THE AWARENESS TRAINING PROGRAM AND IT'S IMPLEMENTATION**

This chapter will propose the ISATP material and will give an overview of some of the techniques we could use to deliver this material. Part A will propose the topics of the ISATP and the justification of why these topics are selected. Part B of this chapter will list the possible techniques for delivering ISATP material. Part C will describe how we are going to evaluate the program and get the feedback from the trainees, lecturers and supervisors. Part D covers the ongoing improvement of the training program.

### **A. PROPOSED AWARENESS TRAINING MATERIAL**

The overall objective for use of this thesis is to facilitate the development of a broad, measurable, cost-effective information security awareness training program which supports the missions of the RSNF. This part of the thesis will propose the topics that comprise the information security awareness training program (ISATP) material. These topics will be essential and need to be well understood by all RSNF employees at all levels. Protecting the RSNF's information assets demands no less. The selection, as I mentioned earlier in chapter three, will be based on the core concepts covered by some of the well-known information security training providers, matched against the needs of the. This proposed material will allow the course developers to have a baseline of subject matter that will comprise the future information security course. The list of the topics included in the proposed material is intended to be fundamental for such type of awareness training, yet it will build a wide range of security-related skills needed by employees in several functional area categories. Moreover, it will be a good starting place for the development of material suitable for training employees with different needs and levels of training. The list will include the topics and a justification of why these topics are important. Although the material framework, presented below, provides a generic outline for material to be included in ISATP training throughout RSNF, it is necessary that the instructor relate the actual course content to the RSNF's unique culture and mission requirements. Emphasis placed on the specific topics may vary by student audience or the specific job needs. [11]

The material framework was developed to present topics and concepts in a logical order, based on information security courses analyzed in chapter three. Appendix E has the full outline of the proposed ISTAP material. Below is a detailed outline that covers the definition of each part, an explanation of why it is important, how it's related to this course, a brief description of the objective of each part, and finally a time estimation needed to cover it:

## 1. Introduction To Information Assurance

### 1.1. INFOSEC & COMPUSEC

1.1.1. Definition: INFOSEC is defined as: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.[12]. COMPUSEC is defined as the application of hardware, firmware and software security features to a computer system in order to protect against, or prevent, the unauthorized disclosure, manipulation, deletion of information or denial of service. [13]

1.1.2. Importance/Relevance: Many people do not really understand what INFOSEC and COMPUSEC are nor what are their goals is. Before we get into the meat of this course, we need to introduce these two concepts to the trainees and make sure they understand them.

1.1.3. Objective: This part will introduce the two concepts of INFOSEC and COMPUSEC; define the two acronyms and how they relate to each other

1.1.4. Time: 30 Minutes

### 1.2. Sensitive Data Definition

1.2.1. Definition: Information that requires some level of protection because its unauthorized disclosure, alteration, or destruction will cause perceivable damage to the institution. [14]

1.2.2. Importance/Relevance: Trainees should know the classification of data and identify the sensitive data that need to be protected and handled with caution; trainees should know the best practices of handling and storing sensitive data.

1.2.3. Objective: Trainees will know which information requires some level of protection because the loss, misuse, or unauthorized access to or modification of, could adversely affect the RSNF or the conduct of its operations, or the privacy of its employees.

1.2.4. Time: 30 minutes

### 1.3. Importance Of Security

1.3.1. Discussion: Information security is a serious issue, and the reason organizations want to protect information should be for sound purposes. Military knowledge and data are arguably the most important assets of any organization. Organizations must ensure the confidentiality, integrity and availability of their data.

1.3.2. Importance/Relevance: The importance of information security to military operations cannot be overstated; Trainees need to realize how important security is to them, their department and the Navy.

1.3.3. Objective: This part will elaborate on the importance of security to organizations in protecting their information and to ensure the unhindered exercise of legitimate activities. Some historical incidents should be presented in this part.

1.3.4. Time: 1 Hour

### 1.4. The Meaning of “secure”

1.4.1. Discussion: Secure means the system is free from vulnerabilities and there are no threats to it.

1.4.2. Importance/Relevance: Trainees should know the meaning of secure, and the fact that security is generally not a 100% achievable, they need to realize that the amount of money spent on protecting an information asset is highly dependant on the value of the information it holds, and the length of time that information needs to be protected. They also need to know that “secure” relates to many things (secure system, secure environment, secure communication...etc).

1.4.3. Objective: Trainees will learn and recognize that secure is a fuzzy word, that total security is far from reality, and that absolute security would mean zero productivity. They will learn that security translates into operating systems in such a way that the residual risk is reduced to an acceptably low level.

1.4.4. Time: 30 Minutes

## 1.5. Security Vulnerabilities

1.5.1. Definition: A security vulnerability is a design flaw in a product that makes it susceptible to an accidental or malicious action that may result in the violation of the security policy (e.g., a user with no clearance is able to view classified information).

1.5.2. Importance/Relevance: Trainees need to know about the vulnerabilities affecting our networks, software, and systems, and how vital it is to stay ahead of the hackers trying to steal our data or disrupt our naval operations.

1.5.3. Objective: For the trainees to obtain a rigorous, quantitative understanding of the vulnerabilities of information systems. They have to be aware of the weaknesses in the way a system or network is set up, operated, or maintained that may make certain information or processes on that system available to unauthorized people who in turn may use these for malicious purposes.

1.5.4. Time: 2 Hour

## 1.6. Threats

1.6.1. Definition: Any circumstances or event that has the potential to cause harm to a system or network [16]

1.6.2. Importance/Relevance: Threats comprise one of the four major terms in the risk management equation discussed in section I where it was shown that residual risk is what is left over after safeguards are applied against the product of threats and vulnerabilities. Thus, threats are a key component in assessing the overall risk any particular system is exposed to. Only by understanding the major threat categories, along with the basic attributes of

each, can those charged with IA duties choose and apply the appropriate safeguards.

1.6.3. Objective: This part is intended to familiarize trainees with the possible threats to the RSNF systems, and will increase their awareness of threats to computer systems by giving a broad picture of the threat environment in which systems are operated today.

1.6.4. Time: 2 Hour

## 1.7. Countermeasures

1.7.1. Definition: Protective measures, techniques, and procedures that must be applied to information systems (IS) and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: 1) Basic: The IS and networks requiring implementation of standard minimum security countermeasures, 2) Medium: The IS and networks requiring layering of additional safeguards above the standard minimum security countermeasures, 3) High: The IS and networks requiring the most stringent protection and rigorous security countermeasures. [17]

1.7.2. Importance/Relevance: As the course will point out, there are risks associated with the operation of computers. In order to operate a computer at an acceptable level of risk, we need countermeasures.

1.7.3. Objective: To introduce trainees to the different countermeasures that would help them to reduce threats, and vulnerabilities, assist in the detection of hostile events, or assist with the recovery from an event and to provide an overview of the effective deployment of countermeasures such as firewalls, intrusion detection systems and virtual private networks. It will enable them to minimize the risks while taking full advantage of the opportunities the information and computer systems affords.

1.7.4. Time: 1 Hour

## 1.8. Policies

- 1.8.1. Definition: A security policy is a document that states in writing how an organization plans to protect the organization's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. An organization's security policy may include an acceptable use policy, a description of how the organization plans to educate its employees about protecting the organization's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made [18]
- 1.8.2. Importance/Relevance: Information security policies are the foundation, the “prime mover” in a manner of speaking, of information security practices and expenditures within an organization. Policy is management's tool for stating WHAT the Information Assurance goals are. As such, policy dictates guidance to security implementers so that they may determine HOW the goals set forth in the policy will be met; typically by choosing appropriate safeguards and by establishing standard security operating procedures.
- 1.8.3. Objective: This part is intended to help the trainees understand a coherent information security policy. It provides a brief overview of the policies applied in different organizations. It discusses the primary uses of the Internet, and the associated policy implications. And it provides sample policy statements for low, medium and high risk/protection environments.
- 1.8.4. Time: 30 Minutes

## 1.9. Assurance

- 1.9.1. Definition: Acts that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[17]

1.9.2. Importance/Relevance: An understanding of assurance is critical because its activities involve many disciplines, and these activities permeate all aspects of using computer and information systems.

1.9.3. Objective: This part discusses assurance perspectives on the underlying technologies, reviews the definition of assurance, and promotes trainees to understand assurance technology and standards impacting real-world needs. This part presents the goals of an information assurance program, explains why meeting these goals are essential to success, and distinguishes between the roles and responsibilities of all members of the organization. This part also explains how to identify and manage risks to information systems.

1.9.4. Time: 2 Hours

## 2. Network Fundamentals

### 2.1. Network Types

2.1.1. Definition: A group of two or more computer systems linked together.

There are many types of computer networks, including 1) local area networks (LANs) 2) Wide area networks (WANs) 3) Metropolitan area network (WANs) 4) Personal area networks (PANs).

2.1.2. Importance/Relevance: A basic understanding of computer networks is requisite in order to understand the principles of network security. Trainees need to have an understanding of the fundamentals of the networks and how they are classified according to their type.

2.1.3. Objective: This part will cover some of the foundations of computer networking, then move on to an overview of some popular networks. The Open Systems Interconnect model (OSI) will be introduced to trainees to make them understand the relationships between OSI, TCP/IP and any generic network protocol stack that employs the layered concept of encapsulation. Following that, this part will take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets. While there are several different network types, this part explains the two most popular types of networks: LANs and WANs.

2.1.4. Time: 30 Minutes

## 2.2. Network Topologies

2.2.1. Definition: The specific physical (i.e., real) or logical (i.e., virtual), arrangement of the elements of a network. We could say that two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types.[19]

2.2.2. Importance/Relevance: Trainees are expected to have a basic understanding of the network topologies, and how the network devices are connected to each other.

2.2.3. Objective: This part will explain the three standard topologies of computer networking 1) Contention-based (bus) 2) Ring, and 3) Switched. Trainees will learn the different layouts of connected devices on a network. It is very important for trainees to fully understand them as they are key elements to understanding and troubleshooting networks and will help them decide what actions to take when they are faced with network problems.

2.2.4. Time: 30 Minutes

## 2.3. Network Devices

2.3.1. Definition: Any part of a network is called a network device; we are interested especially in devices, which forward packets between nodes in a network or between different networks.

2.3.2. Importance/Relevance: The network hubs, switches, and routers provide quite an array of advanced features that interoperate with other network devices. Changes to one device can cause changes to others, these devices are susceptible parts of any network. Trainees thus need to understand these network devices, their functions, and their vulnerabilities to a network.

2.3.3. Objective: The network devices discussed in this part are the hubs, switches and routers, trainees will gain a good understanding of switching and routing technologies. The part will provide a solid understanding of networking devices. This will enable trainees to understand Inter-networks more expediently. In addition, trainees will learn how it is important on critical subnets, to correctly configure network devices: by enabling needed

services, restricting access to configuration services by port/interface/IP address, disabling broadcasts, source routing, choosing strong (non-default) passwords, enable logging, choose carefully who has user/enable/admin access, etc.

2.3.4. Time: 1 Hour

## 2.4. Important Layer 3/4 Network Protocols

2.4.1. Discussion: A set of formal rules describing how to transmit data across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and correction of the bit stream. High level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, sequencing of messages etc.[20]

2.4.2. Importance/Relevance: Trainees should understand the implications of using high-level network protocols operating in an open-system environment.

2.4.3. Objective: The focus of this part is to understand the high-level network protocols, which include layer 3 and 4 protocols IP, TCP, UDP and ICMP). These protocols will be reviewed, but more from the point of view of understanding the properties of various protocols and the practical issues in their use, rather than the technology behind them. General networking will also be covered in order to understand the implications of various approaches; for instance, using UDP (layer 4) vs. TCP (layer 4). Trainees will learn how layer four (transport) transfers data between end systems. End-to-end error recovery and flow control and how layer three (network) provides the addressing scheme necessary for routing packets throughout the network.

2.4.4. Time: 2 Hours

## 2.5. How Packets Get Routed

2.5.1. Discussion: Routing is the technique by which data finds its way from one host computer to another. In the Internet context there are three major aspects of routing 1) Physical address determination 2) Selection of inter-network gateways 3) Symbolic and numeric addresses. [21]

2.5.2. Importance/Relevance: Trainees should have an understanding of a routing configuration that reflects different network topologies and how packets get delivered to their desired destinations.

2.5.3. Objective: This part introduces the underlying concepts widely used in routing protocols. Concepts summarized here include routing protocol components. In addition, it will address specific routing protocols in more detail. In this part trainees will learn about IP datagram and why it is necessary to encapsulate the IP datagram within whatever frame format is in use on the local network or networks to which the computer is attached, and the fact that this encapsulation requires the inclusion of a local network address or physical address within the frame. Moreover, they will learn how local networks interconnected by one or more gateways, generally known as routers. Finally, they will learn how the addresses get translated from a reasonably human friendly form to numeric IP addresses by the Domain Name System (DNS).

2.5.4. Time: 2 Hours

## 3. Computer System Security and Access Controls

### 3.1. System Access Control

3.1.1. Definition: System access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first login to a system, using some Identification and Authentication (I&A) system. [22]

3.1.2. Importance/Relevance: It is essential that trainees be aware of how the access to systems is controlled and how a system administrator can control access to files and folders using system access controls. The importance of

picking a good, secure password cannot be emphasized enough. Until computers are able to recognize people on sight, the primary method of identifying oneself to a computer will remain the password. A password operates much like a key or combination. It is a means of authenticating to the computer that you are who you claim to be. Unfortunately, passwords can be as easily compromised as keys and combinations.

3.1.3. Objective: This part will cover the concepts of identification and authentication and how users are usually identified by a challenge and response system; additionally they will learn the mandatory standard password selection and the purpose of these standards. Students must understand that passwords are often either: a) the only defense or b) the weakest link defense used to protect stronger machine-generated cryptographic keys. They are easily attacked via dictionary or brute-force cracker programs, unless strong passwords are utilized. Students should understand that the "math" is in their favor by explanation of the general combinatorics relation, which will give them brute-force resistant passwords. Students should also be exposed to the good password selection mnemonics; such as using the first letter of an easily remembered phrase, or making letter substitutions (e.g., substituting '5' for 'S').

3.1.4. Time: 1 Hour

### 3.2. Data Access Controls

3.2.1. Definition: Data access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use and content of a system. It permits management to specify what users can do, which resources they can access and what operations they can perform. [23]

3.2.2. Importance /Relevance: Unauthorized access to highly sensitive data can compromise the RSNF data, employee's information, and strategic RSNF information. It is important for trainees to understand how an operating system could be secured using the different access control techniques.

3.2.3. Objective: This part describes the security model for controlling access to application objects, such as files, and for controlling access to administrative functions, such as auditing user actions. The Access-Control topic will provide a high-level description of the access-control components and how they interact with each other. In addition, trainees will learn some of the data accesses control techniques, such as, Discretionary access control (DAC), Mandatory access control (MAC) and access control list (ACL). Trainees need to know that access control (also called protection or authorization) is a security function that protects shared resources against unauthorized accesses and that the distinction between authorized and unauthorized accesses is made according to an access control policy. Moreover, they will know what we mean by objects and subjects in a resource, which are protected by access control. This part will educate trainees that access control is employed to enforce security requirements such as confidentiality and integrity of data resources (e.g., files, database tables), to prevent the unauthorized use of resources (e.g., programs, processor time, expensive devices), or to prevent denial of service.

3.2.4. Time: 1Hour

### 3.3. Access Control Models

3.3.1. Definition: Techniques, which mediate accesses to objects by subjects. The technique may be implemented in hardware or software. There are three popular models that are found in access control systems: 1) Bell & LaPadula where information does not flow to an object of lower classification 2) Clark – Wilson where no subject may depend on a less trusted object or subject 3) Biba where objects of lower integrity are not permitted to flow to objects of higher integrity.

3.3.2. Importance /Relevance: Security models are an important concept in the design of any secure system. A security model is one of the key architectural features that make it an appropriate technology for networked environments.

Security is important because networks represent a potential avenue of attack to any computer hooked to them.

3.3.3. Objective: This part aims to provide trainees with an essential understanding in one of the computer security technologies. This includes high-level issues such as security policy (modeling what ought to be protected). It also involves a review of security policy models. Such as Bell-LaPadula, Clark-Wilson, Biba and Take-Grant Model. In addition, trainees will know how these access controls allow only authorized users, programs or processes system or resource access and how they are granting or denying, according to a particular security model, of certain permissions to access a resource. Moreover, trainees will learn that access control models are an entire set of procedures performed by hardware, software and administrators, to monitor access, identify users requesting access, record access attempts, and grant or deny access based on preestablished rules.

3.3.4. Time: 1 Hour

#### 4. Types Of Attacks

##### 4.1. Probes and Scans

4.1.1. Definition: A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion. Where a scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.[23]

4.1.2. Importance/Relevance: Understanding the real threats to our computers is crucial to formulating an effective computer security plan. It is important for trainees to know about probing and scanning since they are an early warning of a potential follow-on act against the system.

4.1.3. Objective: Trainees will be introduced to the concepts of probing and scanning and how they are used by the attackers to find any vulnerability in our systems. Trainees will learn how to use the network probing or scanning tools to test a network for weaknesses that attackers might exploit. And how a probing or scanning test can be conducted using one of two approaches: black-box (with no prior knowledge of the infrastructure to be tested) and white-box (with a complete knowledge of the network infrastructure).

4.1.4. Time: 30 Minutes

## 4.2. Account Compromise

4.2.1. Discussion: An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has).[23]

4.2.2. Importance/Relevance: Ramifications from an account compromise can range from annoying to catastrophic. If an attacker gets hold of a user account, the system can be compromised in a way that we might not notice. Account compromise might expose systems to serious data loss, data theft, or theft of services.

4.2.3. Objective: In this part trainees will learn how it is important to keep their accounts safe from being compromised, what are the possible drawbacks of losing someone's account. Trainees should recognize that computer security relies on secret passwords. These passwords must be adequately safe against 'cracking' programs that attempt to guess them. They must be kept secret - and thus must not be shared among users. In order to insure that trainees must keep them secret and not to transmit them unencrypted across the network.

4.2.4. Time: 30 Minute

### 4.3. Packet Sniffing

4.3.1. Definition: Packet sniffing is the process of capturing data from information packets as they travel over the network using a packet sniffer program. That data may include user names, passwords, and proprietary information that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffing programs, intruders can launch widespread attacks on systems. Installing a packet-sniffing program does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise. [24]

4.3.2. Importance/Relevance: One of the oldest methods of stealing information off a network is through packet sniffing. Intruders may gain unauthorized access to machines and plant "packet sniffers" on them. Packet sniffing, which has been around since the invention of Ethernet, has legitimate uses. Today, however, the threat of misuse of these programs has increased greatly because they can be downloaded readily via the Internet.

4.3.3. Objective: This part will enlighten the trainees to packet sniffing in computer networks, what we mean by packet sniffing, and what it takes to sniff a packet from a network. Finally, an explanation of how these sniffed packets might be used to exploit our network. Trainees will also learn how a packet sniffer can be legitimately used to capture, monitor and analyze network traffic; detect bottlenecks and other network related problems. Moreover, how a network manager using this information, can keep traffic flowing efficiently.

4.3.4. Time: 30 Minute

### 4.4. Denial of Service

4.4.1. Definition: A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all

network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.[24]

4.4.2. Importance/Relevance: Today's complex network environments and Web hosting systems, vulnerable to break-ins and disruptions. Denial-of-Service (DoS) attacks, in which legitimate users are denied access to Web servers and target systems, can pose especially serious problems for RSNF. It is important that trainees know about the most common type of attacks to networks (Denial-of-service attacks) which can disrupt or completely disable their network.

4.4.3. Objective: This part provides a general overview of attacks in which the primary goal of the attack is to deny the victim(s) access to a particular resource. It should include information on how trainees can help and respond to such an attack. It aimed to have trainees understand that a denial of service (DoS) attack is not a virus but a method hackers use to prevent or deny legitimate users access to a computer and that not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Trainees will also learn that Denial-of-service attacks come in a variety of forms and aim at a variety of services types, some of these attacks will be explained in this part.

4.4.4. Time: 1 Hour

#### 4.5. Spoofing

4.5.1. Definition: A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.[25]

4.5.2. Importance/Relevance: Spoofing attacks are difficult to detect. They are becoming more and more popular now. An improperly configured firewall will allow all traffic from any computer with a spoofed source IP address, which could result in a security vulnerability. Trainees need to completely understand how the spoofing attacks can take place, and what are the possible affects of these attacks to the Navy.

4.5.3. Objective: This part from the ISATP describes the use of IP spoofing as a method of attacking a network in order to gain unauthorized access. Trainees will learn the TCP and IP authentication process and then how an attacker can spoof the network. Trainees will learn that Spoofing is mostly done when the attacker is engaging in DoS type of attack – that is, he just wants to disrupt you and does not expect or need data to return to him. They should realize that the only way to prevent these attacks is to implement security measures like encrypted authentication to secure your network

4.5.4. Time: 30 Minutes

#### 4.6. Malicious Software “Malware”

4.6.1. Definition: Malicious software is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious software includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some

action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.[23]

4.6.2. Importance/Relevance: The danger presented today by malicious software to our Navy's computer-based, mission-critical systems is greater than ever. The number of malicious code incidents continues to climb and trainees need to aware of the increasing "malware" threats and specific defensive techniques to combat malicious software.

4.6.3. Objective: This part examines malicious software detection and malicious software defenses. Viruses, worms and Trojan horses, will be discussed. Trainees will review some of the well-known viruses and worms to understand how they affected the world economy. Upon completing this part trainees will be able to define malware and identify its various forms, explain how viruses, worms, Trojan horses and other types of malware work, describe the ways that malware can harm information assets. Moreover, they will be able to describe ways to prevent, detect, and respond to a malware incident, Explain how anti-virus programs work, and distinguish hype and hoaxes from real malware threats.

4.6.4. Time: 2 Hours

#### 4.7. Social Engineering

4.7.1. Definition: An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system. [26]

4.7.2. Importance/Relevance: Social engineering can be used to gain access on any system despite the platform or the quality of the hardware and software present. It is the hardest form of attack to defend against because hardware and software alone will not stop it. With the immeasurable security threat that Social Engineering brings to the computing community, trainees need to be familiar with these types of attacks.

4.7.3. Objective: This part will discuss the basics of social engineering by giving a general overview of social engineering. It will then discuss what makes

social engineering so successful. It aimed to make trainees aware of the preparation an attacker may go through, and how this can be made difficult by appropriate security measures.

4.7.4. Time: 30 Minutes

## 5. Intrusion Detection

### 5.1. Network Based

5.1.1. Definition: A network-based IDS watches live network packets and looks for signs of computer crime, network attacks, network misuse and anomalies. When it observes an event, it can send pages, email messages, and record it for future forensic analysis.[27]

5.1.2. Importance/Relevance: With the growing reliance on network-based services and the Internet, organizations are faced with a growing challenge to protect their systems from attacks. IDSs are the latest and most powerful tools used for alerting the analyst to network-based exploits. Therefore, trainees are required to have some knowledge on the intrusion detection systems IDSs.

5.1.3. Objective: This part offers a quick start in intrusion detection. It will provide trainees with knowledge on how attackers break into systems and networks, and how a network-based IDS can play a key role in detecting these events within a network. They will also learn how a network-based IDS can be used to determine what exploits are occurring in their network.

5.1.4. Time: 1 Hour

### 5.2. Host Based

5.2.1. Definition: Host-based ID involves loading a piece or pieces of software on the system to be monitored. The loaded software uses log files and/or the system's auditing agents as sources of data.[27]

5.2.2. Importance/Relevance: IDS is a key component and an important tool in computer and network security, just like the previous part of this section,

trainees need to know the different types of ID systems and what are the major pros and cons of each one of them.

5.2.3. Objective: This part will cover the ins and outs of a host-based intrusion detection system. Trainees will learn how a host -based IDS operates and the trade-offs of using it alone.

5.2.4. Time: 30 Minutes

### 5.3. Passive Response

5.3.1. Discussion: Passive IDS will simply alert that an attack maybe happening and provide the data to start investigating.

5.3.2. Importance/Relevance: Most of the intrusion detection systems fall into this category. Trainees need to be aware that most of the old IDS systems are passive and will only report an exploit regardless of the type of IDS (network-or host- based) used to detect it.

5.3.3. Objective: In this part, trainees will be introduced to the passive IDSs and how they work and what they can and cannot do.

5.3.4. Time: 30 Minutes

### 5.4. Active Response (IDP)

5.4.1. Discussion: An active IDS will instead of only sending an alert will also react in some way, this can be reconfigure a packet filtering device, kill a connection, lock a user account etc

5.4.2. Importance /Relevance: Response capabilities for threats and attacks are crucial for any intrusion detection system. Most network-based and host-based IDSs share common threat and attack response options.

5.4.3. Objective: The aim of this part is to make trainees understand the role of an IDP and how it differs from the normal IDSs. Trainees need to realize that firewalls can limit the ability of external hackers to attack IT services, but if they want to secure their systems fully then they will need additional levels of protection for Intrusion Detection and Prevention (IDP). They should realize that a firewall by itself is not enough.

5.4.4. Time: 30 Minutes

## 6. Traffic Filtering (Firewalls)

### 6.1. Types of Firewalls

6.1.1. Definition: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques: 1) Stateless, 2) Statful, 3) Dynamic, 4) Proxy based, 5) Network based, and 6) Host based (Personal).[25]

6.1.2. Importance/Relevance: With the increased connectivity to the Internet and the wide availability of automated cracking tools, organizations can no longer simply rely on operating system security to protect their valuable corporate data. The firewall has emerged as a primary tool used to prevent unauthorized access.

6.1.3. Objective: In this part, trainees will gain experience on firewalls. How they allow access to key services while maintaining our Navy's security, as well the underlying theory and the practical application of a firewall system. By the end of this part, trainees will understand how a firewall works, identify types of firewalls, and choose a suitable firewall system.

6.1.4. Time: 2 Hours

### 6.2. Firewall Configurations

6.2.1. Discussion: A rule-set that specifies what services to let through a firewall, and which ones to keep out. A rule defines the parameters against which each connection is compared, resulting in a decision on what action to take for each connection. The firewall configuration is a complex activity. The complexity depends on the network topology and the security policy desired. Firewall configurations vary from organization to organization. Most often, the firewall consists of several components that can be configured in different ways.

6.2.2. Importance/Relevance: With network security becoming such a hot topic, a trainee might be assigned to implement or reassess a firewall configuration.

6.2.3. Objective: In this part, trainees will be introduced to some common firewall configurations and some best practices for designing a secure network topology. At the end of this part trainees will be familiar with the most common firewall configurations and how they can increase security.

6.2.4. Time: 2 Hour

## 7. Cryptography

### 7.1. Algorithms

7.1.1. Definition: The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.[25]

7.1.2. Importance/Relevance: As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. The use of cryptography is no longer a privilege reserved for governments and highly skilled specialists, but is becoming available for everyone to make use of.

7.1.3. Objective: The objective of this part is to introduce the fundamentals of cryptography to trainees; specifically it will present basic terminology and concepts and describe how cryptography can be used to safeguard the confidentiality, authenticity and integrity of information. Trainees will learn the history and state-of-the art in cryptography, the relationship between cryptography and security, gain experience with basic encryption techniques including symmetric (DES,3DES), asymmetric (RSA, Elliptic curve) ciphers, hashing and how cryptography is used to authenticate the originator of information.

7.1.4. Time: 2 Hours

## 7.2. PKI

7.2.1. Definition: Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI.[25]

7.2.2. Importance/Relevance: A public key infrastructure (PKI) is an increasingly critical component for ensuring privacy and authentication in an enterprise. This technology is capable of securing a wide range of applications across our Navy. Successful PKI deployment requires detailed knowledge of it.

7.2.3. Objective: In this part, trainees will learn how certificate authority (CA) and public key infrastructure (PKI) technologies could be used to ensure the safety of their information assets. They will also evaluate the pros and cons of public and shared keys and define digital certificate, furthermore, they will drill down to the elements of a PKI, including certification authority, key backup and recovery and certificate revocation. They will discover why each piece is essential; learn how each one integrates into a PKI solution, review PKI implementation strategies and new developments. Finally, trainees will gain knowledge of digital signatures and how they can create them using a PGP program.

7.2.4. Time: 2 Hours

## 8. Steganography

8.1.1. Definition: Steganography (from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Steganography takes cryptography a step farther by hiding an encrypted message so that no one

suspects it exists. Ideally, anyone scanning the data will fail to know it contains encrypted data.[25]

8.1.2. Importance/Relevance: Steganography is destined to become more important as more people join the Cyberspace revolution and as the existing governments of the world attempt to regulate or prohibit the use of cryptography for personal privacy purposes.

8.1.3. Objective: This part introduces steganography by explaining what it is, providing a brief history with illustrations of some methods for implementing steganography, and comparing available software providing steganographic services. Trainees need to know that steganography has its place in security. In addition, they it is important for them to recognize that it is not intended to replace cryptography but supplement it. They will learn how hiding a message with steganography methods reduces the chance of detecting that message. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

8.1.4. Time: 30 Minute

## 9. System Hardening

### 9.1. Patches

9.1.1. Definition: A program that corrects a problem with or adds additional features to a particular software title. A patch is not a complete program by itself; it requires a version of the software already on a system. System hardening is a systematic process of securely configuring a system by adding patches to protect it against unauthorized access, while also taking steps to make the system more reliable. Generally anything that is done in the name of system hardening ensures the system is both secure and reliable.[28]

9.1.2. Importance/Relevance: Due to the complexities involved, the process of hardening systems and network servers is frequently not undertaken. Often, users do not realize that the new machine they have deployed is hosting network services that are open to misuse. In any case most network operating systems and servers are typically deployed in the default configuration, which leaves them vulnerable. System hardening can greatly

reduce our vulnerability to misuse from the Internet and our internal network.

9.1.3. Objective: This part describes the importance of hardening our systems by adding the new patches from vendors. Trainees should realize that system hardening is necessary since some operating systems tend to be designed and installed primarily to be easy to use rather than secure. Trainees will recognize that if we harden our systems we can have more confidence in the integrity of our data, performance improvements can be experienced since unnecessary services are removed and inefficiencies in system configuration are detected.

9.1.4. Time: 30 Minutes

## 9.2. Principle of Least Privilege Configuration

9.2.1. Definition: The security guideline that a user should have the minimum privileges necessary to perform a specific task. This helps to ensure that, if a user is compromised, the impact is minimized by the limited privileges held by that user. In practice, a user runs within the security context of a normal user. When a task requires additional privileges, the user can use a tool such as Run as to start a specific process with those additional privileges or to log on as a user with the necessary privileges.[28]

9.2.2. Importance/Relevance: There exists in the field of security the notion of performing tasks with just enough capability, or privilege, to get the job done, and no more. The principle of least privilege means that only the privileges the object needs to perform is assigned tasks. Least privilege is an important principle in countering attacks and limiting damage. POLP is extremely fundamental. It is applicable to every area of security: physical, personnel, communications, computer, networks, data, etc...) It should be applied to the maximum extend possible whenever and wherever possible.

9.2.3. Objective: This part will enable trainees to know the principle of least privilege concept, what does it mean and what it protects from. Trainees will learn how the principle of least privilege is considered important for meeting

integrity objectives. They will learn how to ensure the least privilege that a user given by identifying what the user's job. In addition, they will learn the importance of denying transactions that are not necessary for the performance of the user's duties; and that these denied privileges cannot be used to circumvent the RSNF security policy.

9.2.4. Time: 30 Minute

## 10. Redundancy/Duplication Protection

### 10.1. Data Backups and Types

10.1.1. Discussion: Data backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. Backup is usually a routine part of the operation of large businesses with mainframes as well as the administrators of smaller business computers. For personal computer users, backup is also necessary but often neglected. The retrieval of files we backed up is called restoring them.[24]

10.1.2. Importance /Relevance: Because data is the heart of our Navy and any organization, it is crucial for everybody to protect it. To protect our Navy's data, we need to implement a data backup and recovery plan.

10.1.3. Objective: The primary objective of this part is to allow trainees to obtain an understanding of the underlying importance of data backup, the three different types of backup will be explained in this part, these types include 1) full 2) sequential 3) differential. Trainees will learn when to use what type of these three data backups. In this part trainees will be taught how to choose a backup device, a backup routine, perform timely backups, verify and validate backups and then document and archive backups

10.1.4. Time: 1 Hour

### 10.2. Redundant Systems

10.2.1. Definition: Redundant describes computer or network system components, such as hard disk drives, servers, operating systems, switches, and telecommunication links that are installed to back up primary resources in case they fail.[24]

10.2.2. Importance/Relevance: Where it is inappropriate for networking, computer systems or data to be unavailable for the Navy's critical systems, or it would be impossible for recovery to occur, redundant networking, computer systems and data storage must be in place.

10.2.3. Objective: This part is intended for trainees to appreciate the importance of having redundant systems for the RSNF networks, and how these redundant systems could backup their networks. They will also learn the important parts of a network that need to be backed up by a redundant system, additionally, by the end of this part trainees could rationalize why these redundant systems should not be considered an extra cost to any IT project.

10.2.4. Time: 30 Minute

## 11. E-mail Security

11.1. Discussion: The risks associated with the use of e-mail. The risks include information leakage, data integrity violations, repudiation, malicious code, SPAM, and others and how to mitigate these risks.

11.2. Importance/Relevance: Email is a vital communications channel for organizations of all kinds. As a result, email systems have become an even more important component of their information infrastructure. Nevertheless, with the significant growth of spam, viruses and other types of email attacks it is more challenging to manage and protect this critical communications asset. Most email related security breaches arise directly or indirectly from lack of awareness or knowledge.

11.3. Objective: This part covers the safer use of email services and how to implement security settings and features. The variety of potential threats posed by email services is also reviewed. Trainees will also learn the configurations and settings, as well as the use of an anti-spamming tool. By the end of this part trainees should understand how email works, identify types of email threats, how to defend themselves against email threats using security features in an email application finally they will be introduced to some email security tools.

11.4. Time: 1 Hour

## 12. Laptop\ PDA Security

- 12.1. Discussion: Laptop and PDA security can be broken down into two phases: physical security and access control/authentication.
- 12.2. Importance/Relevance: Laptop computers and PDAs are popular these days and have become a prime target of thieves. These thieves are not only targeting these devices for the value of the device itself, but also for the sensitive data contained therein.
- 12.3. Objective: This part will describe methods trainees can use to protect their laptops and PDAs against physical and data theft. It will discuss technical measures for protecting information on these devices if it is stolen or entered covertly, and notes special problems relating to traveling with these devices.
- 12.4. Time: 1 Hour

## 13. Modem Security

- 13.1. Discussion: MOdulator DEModulator. A piece of communications equipment, which enables a computer to send transmissions through analog telephone lines.
- 13.2. Importance/Relevance: Modems when connected to the Internet pose a great threat to systems and networks. Users with dial-up Internet access from their desktops are the second-biggest security risk in corporations after internal hacking, according to Mark Graff, network security architect at Sun Microsystems.
- 13.3. Objective: Modems and other high-speed connections are becoming increasingly more available. Trainees will learn the security breaches related to the use of a modem to get an internet connection within the Navy's network.
- 13.4. Time: 1 Hour

## **B. TECHNIQUES FOR DELIVERING THE AWARENESS TRAINING MATERIAL**

To be effective, a security program like ISATP must be supported by trained personnel who understand all aspects of information security as it pertains to the RSNF operations. Such critical preparation cannot be obtained in a “one size fits all,” “off-the-shelf” educational program. It’s recognized that professional trainers produce professional results, therefore we have to select and prepare a group of trainers who have a full understanding of the RSNF’s daily operations and have sufficient experience in information security. The selected group will then be enrolled in one of the information security courses offered by either a commercial company or governmental organization. The benefit of this “training the trainer” process will be to have trainers with a solid foundation of skills and knowledge in information security.

To successfully implement a security awareness training program for RSNF end-users we should use internal resources. In RSNF we have several methods of training, and we should identify the best method for achieving the ISATP goals. The good thing about these methods is that the implementation costs associated with them are mostly time related, as awareness-level training is not dependent upon an extensive lab/equipment infrastructure. Individuals learn in different ways, and each has a preferred or primary learning style. The teaching approach most effective for individuals is a function of their preferred learning style, education, and prior experience. In learning information or concepts, some students will do better through reading; others prefer to listen to a lecture, whereas others need to participate in a discussion in order to understand the material. ISATP Instructors should be aware of these learning style differences and should use a variety of teaching approaches and presentation formats, including classroom instruction, computer-based instruction, manuals, self-paced instruction books, and videotapes. [29]

Despite the fact that ISATP delivery should be multi-faceted, this thesis will not propose ISATP material that are suitable for all these formats and delivering techniques mentioned earlier in this chapter. We should also realize that specific formats may be particularly well suited to some circumstances, for example, the training technique used to train a ship crew is likely to be different from the training technique used to train another group in a shore facility, due to the obvious issue of trainee availability. I think that the key

to effective training is to find the right mix of delivery styles for each unique situation; yet it would be great if we can offer ISATP in all the delivery techniques and afford the training to everybody in the RSNF. Some of the available delivery techniques include:

<b>Technique</b>	<b>Definition</b>	<b>Example/Uses</b>	<b>Advantages</b>	<b>disadvantages</b>
<b>Web-Based Training (WBT)</b>	Self-paced, interactive training available on the Internet.	Employees need to access “just in time and just enough” training at the time of the need.  Employees may be working on varying platforms (Windows, Macintosh, and Unix).	Allows easy access anytime and virtually anywhere.  Allows simple update to content.  May use a variety of multimedia effects to draw the user in.  May be linked to resources outside of the course.	Requires computer and Internet access.  Requires self-motivation to complete the training.
<b>Multimedia-based Training (MBT)</b>	Self-paced interactive training presented on a CD-ROM using a variety of multimedia (e.g., audio and video).	Employees are geographically dispersed or otherwise unable to attend scheduled training.  Employees may be unable to access the Internet.	Allows easy access to training on a desktop or laptop.  Does not need access to the Web.	Is not able to take advantage of the power of the Web.
<b>Online Help</b>	Quick and immediate access to information about a specific task delivered to a user at the user’s request.	Users need quick access to information or a quick refresher to get the job done.  Users need a quick cue, tip, or prompt when they roll the mouse over a screen area.  Users need an online tutorial that can be attached to the application.	Allows user to get help and keep working.	Allows limited detail.
<b>Distance Learning</b>	An instructor-led approach where the instructor and participant are separated by place or time.	An instructor posts lessons and exercises, and participants work independently yet have regular online chats with the instructor.  Employees are scattered geographically.  Schedules prevent employees from attending face-to-face training.	Avoids costly travel for geographically scattered employees.  Avoids the need to be physically in a classroom.  Provides some interaction between the instructor and participants.	Allows limited interaction with other participants and the instructor.
<b>Reference Documentation</b>	Factual or procedural information that supports a person doing a particular job after initial learning has occurred.	Information includes job aids, charts, posters, user manuals, and reference guides.	Helps sustain learning.  Serves as ongoing reference.  Allows users easy access to structured information.	No interaction. boring

Technique	Definition	Example/Uses	Advantages	disadvantages
Face-to-face Training	An interactive, instructor-led approach where the instructor and employee meet in a classroom for a specific duration of time in a common location.	Participants benefit from practice and feedback. Subject matter requires a classroom or laboratory situation.	Allows participant and instructor to carry on detailed conversations about unclear points.	Requires participants to travel to a certain location during a particular time period.

Table5. Training Delivery Techniques. From Ref. [30]

## C. EVALUATION AND FEEDBACK

The ability to track and measure results of any training program is of highest importance to our Navy, so we can ascertain the effectiveness of the training program and analyze the return on investment. Therefore, we should offer an effective means for this training program to easily develop surveys, which can be attached to published training materials, and returned to the Information and Computer Department for processing of results. The results can be reviewed by the publishers to evaluate the effectiveness of the materials, and thus offer a means for measuring the return on investment. Practical evidence such as feedback from presenters, audiences, and supervisors is one of the most useful sources of measurement and evaluation of the program. Aspects of the ISATP that can be measured include:

- Audience satisfaction - this can be measured after-the-fact with course or presentation evaluations or surveys about the awareness training program. Evaluations, where the audience is asked to rate the program or activity on a scale, measure how well the audience liked the course, activity, or materials. User feedback may be requested on the relevance and the effectiveness. Asking for suggestions is also a good approach.
- What information the audience has learned (i.e., learning or teaching effectiveness). This can be measured with behavioral objective testing. Pre/post tests and surveys are useful in determining what the audience remembered. Unless a pre-test or preliminary survey is conducted, measuring change is difficult.

- Skill transfer /audience performance. This type of evaluation goes beyond the learner to gather input from an outside evaluator, such as a supervisor, security / incident response personnel, or help desk personnel. Follow-up interviews, walk-through testing, help desk / incident reporting statistics, and audit findings can be used to measure improvements in awareness and job performance. Improvements are measured by comparing pre- and post-test or survey scores.[31]

#### **D. ONGOING IMPROVEMENT**

The training department needs to complete a formal rating evaluation after each course and at the end of the training year to indicate their satisfaction with the training experiences and outcomes, quality of material provided, and facilities and resources available. The Information and Computer Department will review the training satisfaction ratings and take reasonable steps to address any areas of concern. Interviews with the ISATP teachers by the training officers will be completed at the end of the training year to gather additional feedback about the training experience in order to facilitate the continuous improvement of the information security awareness training program (ISTAP). It is expected that the program teachers will provide feedback to program supervisors in training department on an ongoing basis, as well, concerning their needs and the extent to which the training activities are fulfilling their goals. This ongoing feedback process, which will continue for the next program year, will enable the Information and Computer Department to incorporate mid-course changes as needed. The cumulative results of this year's evaluations will provide information on the effectiveness of the ISATP program on the RSNF employees' skills, attitudes, and behavior; as well as the effectiveness of the lecturers' instructional styles.

## **V. CONCLUSION AND RECOMMENDATION**

### **A. CONCLUSION**

For many organizations, taking a long, hard look at information assets and what is being done to protect them has become as important as adding new systems. And knowing how to protect information assets is rapidly becoming one of the most critical educational needs of the new century. Information security training is essential to safeguard operations continuity, minimize the potential risk from damage, avoid and reduce the impact of security related incidents. Effective Information Security training will enable RSNF employees to share data in a more secure environment, whilst ensuring the protection of systems and other RSNF IT resources. Computing facilities and the information systems they support have become increasingly accessible as a result of the explosion of the open, public internet and the expanded use of the computer systems in all aspects of operations in the RSNF. A great deal of attention is now being focused on this issue. Regrettably this attention was not followed by actions to elevate the RSNF employees to an acceptable level of security awareness training.

Security awareness training pushed by the modern-threats to computers and systems, the necessity of having a more secure working environments in the Navy and the mixing of various security responsibilities to each and everyone in the RSNF, led to the need of developing an awareness training program for the RSNF. The purpose of this thesis has been to evaluate some of the existing information security courses offered by some commercial company's and educational institutions, this evaluation helped to select the appropriate material that best fit the needs of the RSNF.

The Information Security Awareness Training Program (ISATP) provides detailed, specific information to help the Saudi Navy in starting a basic course to train its employees in Information Assurance (IA). RSNF should measure the effectiveness of the ISTAP and the extent to which this program is useful to the Navy and are sensible spending of training resources. As this thesis has shown, security training is intended to all RSNF employees with all different responsibilities they might have, everyone with a computer connected to a network is exposed to situations that might require some sort of training that bring forth an

appropriate response. For this reason, the ISATP material covers a broad-spectrum of IA, to meet the needs of the mixture backgrounds and expertise among the trainees', this program will serve as a solid foundation for the RSNF employees and to make them knowledgeable of their role in protecting the Navy's information. There is certainly more to be done, however. I consider this thesis the first step of what I hope will be an extended study of information security training in the future.

## **B. RECOMMENDATIONS FOR FUTURE WORK**

This thesis did not attempt to solve the entire problem of not having an information security training program in the RSNF, yet it makes the first move toward having such a program, this move is intended to help the RSNF IT personnel in developing a basic ISATP to train all the RSNF employees. This thesis is advisory and not directive. It provides guidance on specific requirements that may influence the strategies of developing, delivering and implementing ISATP to the Navy. This thesis does not establish or originate the complete ISATP. Instead, its purpose is to clarify the importance, essential contents and depth of coverage of a complete ISATP. Methods described in this thesis represent recommended approaches to meet RSNF security requirements; RSNF may choose other approaches that provide assurance that these requirements are met. However, recommended approaches and criteria set forth in this thesis for the development, delivering, and implementation of security training may be used as the basis for building a comprehensive ISATP.

It was shown that in order to train the vast majority of the RSNF employees we need to consider the different delivering techniques available to solve the problem of trainee's availability. Further research into proposing materials suitable for the different techniques enclosed in chapter four of this thesis is recommended for future studies. In addition to the suitability of the proposed material to the delivering techniques, these materials should be designed to fulfill the unique RSNF security training needs such as training the network administrators and information security officers. It is also recommended that additional research be done on providing a computer lab with all the tools needed for such training;

these tools may include (password cracking software, intrusion detection systems, firewalls, and Steganography tools....etc).

Another central and important issue deserving further study is the examination of the effectiveness of the ISTAP program. This study should also address the need to keep the ISATP current and relevant. Such ongoing evaluation is an essential component of any training program. This is especially true in sensitive fields such as information security, where the recipients of the training directly affect the operations of the Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX A - SANS TRACK 1 COURSE OUTLINE

This appendix is provided to list the terminologies and core concepts covered in: Security essentials course.

<b>DAY</b>	<b>Topic</b>	<b>Terminologies and core concepts covered</b>
<b>Day 1</b>	<b>Network Fundamentals</b>	Network Types (LANs, WANs) Network Topologies Ethernet, Token Ring ATM, ISDN, X.25 Wireless Wiring Network Devices VLANS Voice over IP
	<b>Network Layer Security Protocols</b>	IPSec SKIP SWIPE
	<b>Application Layer Security Protocols</b>	S/MIME SET PEM
	<b>IP Concepts</b>	Packets and Addresses IP Service Ports IP Protocols TCP UDP ICMP DNS
	<b>IP Behavior</b>	TCPdump Recognizing and Understanding UDP ICMP UDP Behavior
	<b>IOS and Router Filters</b>	Routers IOS Routing Routing Protocols Access Control Lists
	<b>Host-based Perimeter Protection</b>	Vulnerabilities Four Primary Threats Personal Firewalls
	<b>Physical Security</b>	Facility Requirements Technical Controls Environmental Issues Personal Safety Physical Security Threats Elements of Physical Security
	<b>Hardware Architecture</b>	Memory Types Machine Types Operating System States Storage Types Operating System Protection Mechanisms
<b>Day 2</b>	<b>Information Assurance Foundations</b>	Threat Model Authentication vs. Authorization Data Classification Vulnerabilities Defense In-Depth
	<b>Computer Security Policies</b>	Elements When Well Written How Policies Serve as Insurance Roles and Responsibilities

<b>DAY</b>	<b>Topic</b>	<b>Terminologies and core concepts covered</b>
	<b>Contingency and Continuity Planning</b>	Legal and Regulatory Requirements Disaster Recovery Strategy and Plan
	<b>Business Impact Analysis</b>	Emergency Assessment Business Success Factors Critical Business Functions
	<b>Password Management</b>	Password Cracking for Windows and Unix Alternate Forms of Authentication (Tokens, Biometrics) Single Sign On and RADIUS
	<b>Access Control Techniques</b>	Discretionary Access Control (DAC) Mandatory Access Control (MAC) Lattice, Rule and Role Based, and Tokens/Tickets
	<b>Access Control Modes</b>	Bell LaPadula (BLP) Biba, Clark Wilson and Non-Interference State Machine and Information Flow
	<b>Access Protocols</b>	CHAP PAP
	<b>Incident Handling</b>	Preparation, Identification and Containment Eradication , Recovery and Lessons Learned Evidence Handling and Laws Investigation Techniques and Computer Crime Ethics
	<b>Offensive and Defensive Information Warfare</b>	
	<b>Web Security</b>	Web Communication Web Security Protocols Active Content Cracking Web Applications Web Application Defenses
	<b>Data Warehousing</b>	Aggregation and Data Mining Inference, Polyinstantiation and Multi-level Security
	<b>System Development</b>	System Development Life Cycle and Security Control Architecture Service Level Agreements (SLAs) Programming Techniques and Secure Programming Remote Procedure Calls (RPCs), Flaws and Issues
	<b>Types of Systems</b>	Knowledge Based, Expert Systems and Neural Networks
<b>Day 3</b>	<b>Host-based Intrusion Detection</b>	TCP Wrappers, Nuke Nabber, Back Officer Friendly, AtGuard Syslog Tripwire Forensics
	<b>Network-based Intrusion Detection</b>	Commercial Tools CIDF, CVE Shadow
	<b>Methods of Attacks</b>	Brute Force Denial of Service Spoofing Pseudo Flaw Alteration Code Logic Bomb Trap Door Interrupts Inference Traffic Analysis Flooding Spamming
	<b>Honey pots</b>	What They Are and How to Deploy Them Deception Toolkit
	<b>Firewalls and Perimeters</b>	Firewalls and Policy Enforcement Packet Filtering, State Aware and Proxy Intrusion Detection Using Firewall Logs Effect of Firewalls on IDS Sensors Firewall Avoidance Techniques, Modems and Backdoors
	<b>Risk Assessment and Auditing</b>	Introduction to Risk Management Calculation of Acceptable Loss Dollar Driven vs. Qualitative Knowledge Based (Accreditation) Securing NT Step-by-Step Introduction to Auditing Risk Assessment Checklists

DAY	Topic	Terminologies and core concepts covered
		Vulnerability Scanners Common Vulnerability and Initiative Saint Nessus ISS Security Scanner War Dialing Penetration Testing
	<b>Security Policy</b>	How All These Capabilities Work Together Automated Response Chain of Custody and Legal Issues
	<b>Introduction to Information Warfare</b>	Know Your Enemy-Ankle Biters to Full IW Cyberwar in the Real World Cyberwar Scenario
	<b>Future Directions</b>	Where These Technologies are Heading
<b>Day 4</b>	<b>Cryptography</b>	Need for Cryptography Types of Encryption Symmetric Asymmetric Hash Ciphers Digital Substitution Algorithms Real-world Cryptosystems Crypto Attacks VPNs Types of Remote Access PKI Digital Certificates Key Escrow
	<b>Steganography</b>	Types Applications Detection
	<b>PGP</b>	Installing and Using PGP Signing Data and What It Means Key Management Key Servers
	<b>Anti-Viral Tools on Desktops</b>	Malicious Code Virus and Hoax Information Organizational Anti-viral Policy Desktop Anti-viral Care, Feeding, Recovery of Damaged Files and Systems
	<b>Operations Security</b>	Legal Requirements Administrative Management Individual Accountability Need to Know Privileged Operations Control Types Operation Controls Reporting
<b>Day 5</b>	<b>The Security Infrastructure</b>	The Windows Family of Operating Systems Workgroups And Local Accounts What Is Active Directory? Domain Users and Groups Kerberos, NTLMv2, Smart Cards Forests and Trusts What is Group Policy?
	<b>Permissions and User Rights</b>	NTFS Permissions File and Print Sharing Service Shared Folders Encrypting File System Shared Printers The Registry and Registry Permissions User Rights
	<b>Security Policies and Templates</b>	Group Policy Objects Password Policy Lockout Policy Anonymous Access

DAY	Topic	Terminologies and core concepts covered
		Software Restriction Policies NTLMv2 Authentication Protecting Critical Accounts
	<b>Service Packs, Patches and Backups</b>	Service Packs E-Mail Security Bulletins Hotfix Network Checker (HFNETCHK.EXE) Patches Installation Windows and System Update Software Update Services Windows Backups System Restore Device Driver Rollback
	<b>Securing Network Services</b>	The Best Way To Secure A Service Firewalls and Packet Filtering IPSec and VPNs Wireless Networking Internet Information Server (IIS) IIS Lockdown Tool URLSCAN Terminal Services
	<b>Auditing and Automation</b>	Microsoft Baseline Security Analyzer CIS Scoring Tool SECEDIT.EXE Windows Event Logs NTFS and Registry Auditing IIS Logging Creating System Baselines Scripting Tools Scheduling Jobs
<b>Day 6</b>	<b>Patching and Software Installation</b>	The Need for Patches Obtaining and Installing System Patches Managing Third-party Software Apps
	<b>Minimizing System Services</b>	Guidance for Dangerous Services Controlling Services at Boot Time Inetd and xinetd IP-based Access Control
	<b>Logging</b>	Syslog and Other Standard Logs System Accounting Process Accounting
	<b>Warning Banners</b>	Sample Warning Banner Texts Standard Warning Banner Config Banners for Networked Services
	<b>Access Control</b>	Username, UID, the Superuser Blocking Accounts, Expiration, etc. Restricting Superuser Access Boot-level Access Control Disabling .rhosts
	<b>Additional Security Configuration</b>	File System Access Control Kernel Tuning for Security Security for the cron System
	<b>Backups and Archives</b>	tar, dump, and dd Tricks and Techniques Networked Backups

Table2. Terminologies and Core Concepts Covered by SANS Security Essential Course Topics. From Ref. [4]

## APPENDIX B - NPS INFORMATION ASSURANCE (IA): COMPUTER SECURITY COURSE OUTLINE

This appendix is provided to list the terminologies and core concepts covered in NPS Information Assurance (IA): Computer Security Course.

Week	Topic	Terminologies and core concepts covered
Week 1	<b>Section 1: Introduction to Information Assurance Computer Security</b> <b>Section 2: Access Control, Identification &amp; Authentication, and DAC</b>	INFOSEC COMPUSEC Data Secrecy Vice Data Integrity Policies and Assurance Threat Models (Amateur & Professional) Trusted systems Ethics and Computer Security History of Computer Security Information Warfare Cost of security Simple System Access Control Identification and Authentication Passwords and Password Files Password Attacks and Cracking Password Selection LAN Manager (LanMan) Authentication Tokens Biometrics Reply Attacks Challenge and response Protocol Login Spoofing Programs Trusted Path Modems (Legitimate & Illegitimate) Data Access Control Permission Bits Capability List Access Control Lists (ACLs) W2K ACLs
Week 2	<b>Access Control, MAC &amp; supporting policies</b>	Labeled Data Label-Based Policies MAC policies Bell and LaPadula Model (BLP) Compartments and Levels An Integrity Model The Biba Model Covert Channels Storage channels Disk Exhaustion Channel Timing Channel Multilevel Subjects Supporting Policies Limitations of Access Control
Week 3	<b>Building Secure Systems &amp; Assurance Issues</b>	Assurance Vice Policies Terms and Concepts Reference Monitor Protection of Memory Segmentation of Memory Separation of Processes MAC Labeling Protection Domains Intel Privilege Level (PL) Protection Mechanism An Intel Gate Call Ring Brackets Modularity Layering Data –Hiding/ Information Hiding

Week	Topic	Terminologies and core concepts covered
		Analysis Formal Methods Analysis Security Models Medium and High Assurance Use More Security Models
Week 4	Malicious Software & Attacks	Viruses Worms Trojan Horses Backdoors/ Trapdoors Packet Sniffing Buffer Overflow Attacks The Smurf Attack IP Spoofing Ping Command Unix Backdoors Social Engineering
Week 5-6	System Accreditation & Certification	System Evaluation TCSEC (Orange Book) Common Criteria Orange book Requirements CC Requirements EAL Accreditation and Certification Designated Approved Authority ( DAA) Operating Modes DITSCAP System Security Authorization Agreement (SSAA) System Characteristics Certification Levels Certification Analysis Tasks Certification and Evaluation of the Integrated Systems Vulnerability or Risk Analysis Issues Annual Loss Expectancy(ALE) Based Risk Analysis Controls and Safeguards NAVSO PUB 5239-16 Risk Analysis Method Comparisons
Week 6-7	Basics of Cryptography	Terms and Notations Types of Cryptography Keys Conventional Cryptography Public Key Cryptography Caesar Cipher Shift Cipher General Substitution Cipher Polyalphabetic Substitution Ciphers Vigenere Cipher One –Time- Pad Cipher Binary Substitution Ciphers Transposition Permutation Technique Multiple Stage Ciphers Plain Text Attack Confusion Diffusion Advanced Encryption Standard (AES) Digital Encryption Standard (DES) S-Boxes Block Cipher Modes Electronic Code Book Mode(ECB) Cipher Block Chaining Mode(CBC) Output feed Back Mode(OFB) Cipher Feed Back Mode(CFB) Triple DES Other conventional Ciphers Public Key Cryptography Public Key Distribution Public Key Algorithm Rivest-Shamir-Adleman (RSA) Algorithm Conventional Vice Public Key Encryption

Week	Topic	Terminologies and core concepts covered
		Hashing Message Authentication Codes (MACs)
Week 8	Cryptographic Protocols	Services Provided by cryptosystems Protocols Arbitrated Protocol Adjudicated Protocol Self-Enforcing Protocol Integrity Integrity With Conventional Cryptography Integrity Protocol Examples Authentication with Conventional Cryptography Secrecy With Public Key Cryptography Integrity With Public Key Cryptography Authentication With Public Key Cryptography Integrity and Authenticity With Public Key Cryptography Digital Signatures Non-Repudiation Protocol Key Distribution KEY Distribution Center (KDC) Hybrid Scheme and Hybrid Encryption Scheme Timestamps Nonces
Week 9	Network Security I: Basics	Packet Switched Networks Circuit Switched Networks Circuit Vice Packet Switched Networks Network Attacks Threats to Network Security Network Encryption End-To-End Encryption Link Encryption Link Encrypted Network Virtual Private Networks (VPNs) Gateway-To-Gateway VPN Client-To Gateway VPN OSI Reference Model Network Security Policies Network Evaluation
Week 10-11	Network Security II: TCP/IP, Firewalls & Intrusion Detection	TCP/IP IP Protocol TCP Protocol TCP Port Numbers Encapsulation UDP Protocol ICMP protocol Packet Sniffing IP Spoofing Three-Way Handshake Firewalls Static Packet Filters Dynamic Packet Filters Application Gateways Firewall Network Configuration Intrusion Detection Systems (IDSs) Host-Based IDS's Network-Based IDS's Distributed Sensor Systems Honey Pots
Week 11-12	Network Security III Public Key Infrastructure (PKI)	Digital Signatures Public Key Distribution Certificates Certificate Authorities (CAs) Private Key Storage Creation of Certificates X.505 Certificate Standard Certificate Revocation Lists (CRLs)

Table 3. Information Assurance (IA): Computer Security Course. From Ref. [6]

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX C – LTI INTRODUCTION TO SYSTEM AND NETWORK SECURITY COURSE OUTLINE

This appendix is provided to list the terminologies and core concepts covered in Learning Tree International-.

Day	Topic	Terminologies and core concepts covered
Day 1	ESTABLISHING YOUR ORGANIZATION'S SECURITY	<p>Real threats that impact security</p> <ul style="list-style-type: none"> <li>• Hackers inside and out</li> <li>• Masqueraders and counterfeiters</li> <li>• Eavesdropping</li> <li>• Spoofing</li> <li>• Sniffing</li> <li>• Trojan horses</li> <li>• Viruses</li> <li>• Bombs</li> <li>• Wiretaps</li> </ul> <p>A security policy: the foundation of your protection</p> <ul style="list-style-type: none"> <li>• The four objectives: availability, integrity, confidentiality and authenticity</li> <li>• Maximizing threat reduction</li> <li>• Assessing your exposure</li> <li>• Implementing the countermeasures</li> </ul>
	NETWORK INTERCONNECTIONS: A MAJOR POINT OF VULNERABILITY	<p>Basic operating system and TCP/IP concepts</p> <ul style="list-style-type: none"> <li>• Login accounts and passwords</li> <li>• File/directory access permission</li> <li>• Some well-known security gaps</li> </ul> <p>Early system security improvements</p> <ul style="list-style-type: none"> <li>• DES encryption</li> <li>• Shadow passwords</li> <li>• Dialback/dialer passwords</li> </ul>
Day 2	DETECTING MASQUERADERS AND ENSURING AUTHENTICITY	<p>Impersonating users</p> <ul style="list-style-type: none"> <li>• Stealing passwords</li> <li>• “Borrowing” IP addresses</li> </ul> <p>How masqueraders infiltrate a system</p> <ul style="list-style-type: none"> <li>• Brute force guessing</li> <li>• Using crack to discover passwords</li> <li>• Replaying network login exchanges</li> <li>• Planting a Trojan horse</li> </ul> <p>Holding your defensive line</p> <ul style="list-style-type: none"> <li>• Hiding passwords</li> <li>• Implementing packet filters</li> <li>• Adopting strong authentication with Kerberos and other tools</li> <li>• Authenticating users with public key encryption</li> </ul>
	PREVENTING EAVESDROPPING TO PROTECT YOUR CONFIDENTIALITY	<p>Unauthorized listening and looking</p> <ul style="list-style-type: none"> <li>• Peeking at files</li> <li>• Snooping with analyzers &amp; wiretaps</li> </ul> <p>Countering the eavesdropper</p> <ul style="list-style-type: none"> <li>• File and data encryption</li> </ul>

Day	Topic	Terminologies and core concepts covered
		<ul style="list-style-type: none"> <li>• Hiding behind firewalls</li> <li>• Using SSL to maintain Web confidentiality</li> </ul>
Day 3	<b>THWARTING COUNTERFEITERS AND FORGERY TO RETAIN INTEGRITY</b>	<p>The forger's arsenal</p> <ul style="list-style-type: none"> <li>• Hacking e-mail messages</li> <li>• Censoring system logs</li> <li>• Scrambling the routing tables</li> </ul> <p>Shielding your assets</p> <ul style="list-style-type: none"> <li>• Encrypting files and messages</li> <li>• Using digital signatures to protect transactions: PGP/MD5</li> <li>• Protecting logs with immutable files</li> <li>• Adopting advanced routing protocols</li> </ul>
	<b>AVOIDING DISRUPTION OF SERVICE TO MAINTAIN AVAILABILITY</b>	<p>Denial-of-service attacks</p> <ul style="list-style-type: none"> <li>• Delivering viruses and bombs via the Web</li> <li>• Data flooding</li> </ul> <p>Constructing your bastions</p> <ul style="list-style-type: none"> <li>• Smart MUAs</li> <li>• Anti-virus toolsets</li> <li>• Imposing quotas on processes, files and accounts</li> </ul> <p>The importance of firewalls</p> <ul style="list-style-type: none"> <li>• Using a packet filter to shield against bombardment</li> <li>• Using application proxies to manage Internet communications</li> </ul>
Day 4	<b>FIREWALLS AND FIREWALL TOPOLOGIES</b>	<p>Choosing the right firewall</p> <ul style="list-style-type: none"> <li>• Packet filters</li> <li>• Circuit level</li> <li>• socks</li> <li>• Application proxies gateway</li> </ul> <p>Firewall topologies</p> <ul style="list-style-type: none"> <li>• Using supportive technologies to provide “defense in depth”</li> <li>• Creating virtual private networks (VPNs) using firewall-to-firewall encryption</li> <li>• Setting up the “demilitarized zone”</li> <li>• Sitting externally accessible servers</li> </ul>
	<b>DEVELOPING YOUR SECURITY POLICY</b>	<p>Steps to take now</p> <ul style="list-style-type: none"> <li>• Conducting a threat reduction analysis</li> <li>• Determining the appropriate countermeasures</li> <li>• Producing your action plan</li> <li>• Choosing the right tools</li> </ul> <p>Responding to attacks</p> <ul style="list-style-type: none"> <li>• Assigning responsibilities</li> <li>• Limiting damage</li> <li>• Choosing the appropriate response</li> <li>• Keeping up with new vulnerabilities</li> </ul>

Table 4. Learning Tree International- Introduction to System and Network Security Course. From Ref. [7]

## APPENDIX D - LAPTOP SOLUTIONS COMPTIA SECURITY+™ CERTIFICATION EXAM TRAINING COURSE OUTLINE

This appendix is provided to list the terminologies and core concepts covered in Laptop Solutions CompTIA Security+™ Certification Exam Training Course.

Section	Topic	Terminologies and core concepts covered
Sec 1	General Security Concepts	<p>Access Control</p> <ul style="list-style-type: none"> <li>• MAC/DAC/RBAC</li> </ul> <p>Authentication</p> <ul style="list-style-type: none"> <li>• Kerberos</li> <li>• CHAP</li> <li>• Certificates</li> <li>• Username/Password</li> <li>• Tokens</li> <li>• Multi-Factor</li> <li>• Mutual Authentication</li> <li>• Biometrics</li> </ul> <p>Non-essential Services and Protocols –( Disabling unnecessary systems / process / programs).</p> <p>Attacks</p> <ul style="list-style-type: none"> <li>• DOS/DDOS</li> <li>• Back Door</li> <li>• Spoofing</li> <li>• Man in the Middle</li> <li>• Replay</li> <li>• TCP/IP Hijacking</li> <li>• Weak Keys</li> <li>• Mathematical</li> <li>• Social Engineering</li> <li>• Birthday</li> <li>• Password Guessing <ul style="list-style-type: none"> <li>➤ Brute Force</li> <li>➤ Dictionary</li> </ul> </li> <li>• Software Exploitation</li> </ul> <p>Malicious Code</p> <ul style="list-style-type: none"> <li>• Viruses</li> <li>• Trojan Horses</li> <li>• Logic Bombs</li> <li>• Worms</li> </ul> <p>Social Engineering</p> <p>Auditing - Logging, system scanning</p>
Sec 2	Communication Security	<p>Remote Access</p> <ul style="list-style-type: none"> <li>• 802.1x</li> <li>• VPN</li> <li>• RADIUS</li> <li>• TACACS/+</li> <li>• L2TP/PPTP</li> <li>• SSH</li> <li>• IPSEC</li> <li>• Vulnerabilities</li> </ul> <p>Email</p> <ul style="list-style-type: none"> <li>• S/MIME</li> <li>• PGP</li> <li>• Vulnerabilities <ul style="list-style-type: none"> <li>➤ Spam</li> <li>➤ Hoaxes</li> </ul> </li> </ul> <p>Web</p> <ul style="list-style-type: none"> <li>• SSL/TLS</li> <li>• HTTP/S</li> <li>• Instant Messaging</li> </ul>

Section	Topic	Terminologies and core concepts covered
		<ul style="list-style-type: none"> <li>• LTS INFORMATION 7/16/02 1</li> <li>• Vulnerabilities</li> <li>• Naming Conventions</li> <li>• Packet Sniffing</li> <li>• Privacy</li> </ul> <p>Vulnerabilities</p> <ul style="list-style-type: none"> <li>• Java Script</li> <li>• ActiveX</li> <li>• Buffer Overflows</li> <li>• Cookies</li> <li>• Signed Applets</li> <li>• CGI</li> <li>• SMTP Relay</li> </ul> <p>Directory – Recognition not administration</p> <ul style="list-style-type: none"> <li>• SSL/TLS</li> <li>• LDAP</li> </ul> <p>File Transfer</p> <ul style="list-style-type: none"> <li>• S/FTP</li> <li>• Blind FTP/Anonymous</li> <li>• File sharing</li> <li>• Vulnerabilities <ul style="list-style-type: none"> <li>➤ Packet Sniffing</li> </ul> </li> </ul> <p>Wireless</p> <ul style="list-style-type: none"> <li>• WTLS</li> <li>• 802.11x</li> <li>• WEP/WAP</li> <li>• Vulnerabilities <ul style="list-style-type: none"> <li>➤ Site Surveys</li> </ul> </li> </ul>
Sec 3	Infrastructure Security	<p>Devices</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• Routers</li> <li>• Switches</li> <li>• Wireless</li> <li>• Modems</li> <li>• RAS</li> <li>• Telecom/PBX</li> <li>• VPN</li> <li>• IDS</li> <li>• Network Monitoring/Diagnostic</li> <li>• Workstations</li> <li>• Servers</li> <li>• Mobile Devices</li> </ul> <p>Media</p> <ul style="list-style-type: none"> <li>• Coax</li> <li>• UTP/STP</li> <li>• Fiber</li> <li>• Removable media <ul style="list-style-type: none"> <li>➤ Tape</li> <li>➤ CDR</li> <li>➤ Hard drives</li> <li>➤ Diskettes</li> <li>➤ Flashcards</li> <li>➤ Smartcards</li> </ul> </li> </ul> <p>Security Topologies</p> <ul style="list-style-type: none"> <li>• Security Zones <ul style="list-style-type: none"> <li>➤ DMZ</li> <li>➤ Intranet</li> <li>➤ Extranet</li> </ul> </li> <li>• VLANs</li> <li>• NAT</li> <li>• Tunneling</li> </ul> <p>Intrusion Detection</p> <ul style="list-style-type: none"> <li>• Network Based <ul style="list-style-type: none"> <li>➤ Active Detection</li> <li>➤ Passive Detection</li> </ul> </li> <li>• Host Based</li> </ul>

Section	Topic	Terminologies and core concepts covered
		<ul style="list-style-type: none"> <li>➤ Active Detection</li> <li>➤ Passive Detection</li> <li>• Honey pots</li> <li>• Incident Response</li> </ul> <p>Security Baselines</p> <ul style="list-style-type: none"> <li>• OS/NOS Hardening (Concepts and processes) <ul style="list-style-type: none"> <li>➤ File System</li> <li>➤ Updates (Hotfixes, Service Packs, Patches)</li> </ul> </li> <li>• Network Hardening <ul style="list-style-type: none"> <li>➤ Updates (Firmware)</li> <li>➤ Configuration <ul style="list-style-type: none"> <li>- Enabling and Disabling Services and Protocols</li> <li>- Access control lists</li> </ul> </li> </ul> </li> </ul> <p>Application Hardening</p> <ul style="list-style-type: none"> <li>• Updates (Hotfixes, Service Packs, Patches)</li> <li>• Web Servers</li> <li>• Email Servers</li> <li>• FTP Servers</li> <li>• DNS Servers</li> <li>• NNTP Servers</li> <li>• File/Print Servers</li> <li>• DHCP Servers</li> <li>• Data Repositories <ul style="list-style-type: none"> <li>➤ Directory Services</li> <li>➤ Databases</li> </ul> </li> </ul>
Sec 4	Basics of Cryptography	<p>Algorithms</p> <ul style="list-style-type: none"> <li>• Hashing</li> <li>• Symmetric</li> <li>• Asymmetric</li> </ul> <p>Concepts of using cryptography</p> <ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity <ul style="list-style-type: none"> <li>➤ Digital Signatures</li> </ul> </li> <li>• Authentication</li> <li>• Non-Repudiation <ul style="list-style-type: none"> <li>➤ Digital Signatures</li> </ul> </li> <li>• Access Control</li> </ul> <p>PKI</p> <ul style="list-style-type: none"> <li>• Certificates – Make a distinction between what certificates are used for what purpose. Basics only. <ul style="list-style-type: none"> <li>➤ Certificate Policies</li> <li>➤ Certificate Practice Statements</li> </ul> </li> <li>• Revocation</li> <li>• Trust Models</li> </ul> <p>Standards and Protocols</p> <p>Key Management/Certificate Lifecycle</p> <ul style="list-style-type: none"> <li>• Centralized vs. Decentralized</li> <li>• Storage <ul style="list-style-type: none"> <li>➤ Hardware vs. Software</li> <li>➤ Private Key Protection</li> </ul> </li> <li>• Escrow</li> <li>• Expiration</li> <li>• Revocation <ul style="list-style-type: none"> <li>➤ Status Checking</li> </ul> </li> <li>• Suspension <ul style="list-style-type: none"> <li>➤ Status Checking</li> </ul> </li> <li>• Recovery <ul style="list-style-type: none"> <li>➤ M of N Control</li> </ul> </li> <li>• Renewal</li> <li>• Destruction</li> <li>• Key Usage <ul style="list-style-type: none"> <li>➤ Multiple Key Pairs (Single, Dual)</li> </ul> </li> </ul>
Sec 5	Operational/Organizational Security	<p>Physical Security</p> <ul style="list-style-type: none"> <li>• Access Control <ul style="list-style-type: none"> <li>➤ Physical Barriers</li> </ul> </li> </ul>

Section	Topic	Terminologies and core concepts covered
		<ul style="list-style-type: none"> <li>➤ Biometrics</li> <li>• Social Engineering</li> <li>• Environment <ul style="list-style-type: none"> <li>➤ Wireless Cells</li> <li>➤ Location</li> <li>➤ Shielding</li> <li>➤ Fire Suppression</li> </ul> </li> </ul> <p>Disaster Recovery</p> <ul style="list-style-type: none"> <li>• Backups <ul style="list-style-type: none"> <li>➤ Off Site Storage</li> </ul> </li> <li>• Secure Recovery <ul style="list-style-type: none"> <li>➤ Alternate Sites</li> </ul> </li> <li>• Disaster Recovery Plan</li> </ul> <p>Business Continuity</p> <ul style="list-style-type: none"> <li>• Utilities</li> <li>• High Availability / Fault Tolerance</li> <li>• Backups</li> </ul> <p>Policy and Procedures</p> <ul style="list-style-type: none"> <li>• Security Policy <ul style="list-style-type: none"> <li>➤ Acceptable Use</li> <li>➤ Due Care</li> <li>➤ Privacy</li> <li>➤ Separation of duties</li> <li>➤ Need to Know</li> <li>➤ Password Management</li> <li>➤ SLA</li> <li>➤ Disposal / Destruction</li> <li>➤ HR Policy <ul style="list-style-type: none"> <li>- Termination - Adding / revoking passwords, privileges, etc.</li> <li>- Hiring - Adding / revoking passwords, privileges, etc.</li> <li>- Code of Ethics</li> </ul> </li> </ul> </li> <li>• Incident Response Policy</li> </ul> <p>Privilege Management</p> <ul style="list-style-type: none"> <li>• User/Group/Role Management</li> <li>• Single Sign-on</li> <li>• Centralized vs. Decentralized</li> <li>• Auditing (Privilege, Usage, Escalation)</li> <li>• MAC/DAC/RBAC</li> </ul> <p>Forensics (Awareness, conceptual knowledge and understanding – know what your role is)</p> <ul style="list-style-type: none"> <li>• Chain of Custody</li> <li>• Preservation of Evidence</li> <li>• Collection of Evidence</li> </ul> <p>Risk Identification</p> <ul style="list-style-type: none"> <li>• Asset Identification</li> <li>• Risk Assessment</li> <li>• Threat Identification</li> <li>• Vulnerabilities</li> </ul> <p>Education – Training of end users, executives and HR</p> <ul style="list-style-type: none"> <li>• Communication</li> <li>• User Awareness</li> <li>• Education</li> <li>• Online Resources</li> </ul> <p>Documentation</p> <ul style="list-style-type: none"> <li>• Standards and Guidelines</li> <li>• Systems Architecture</li> <li>• Change Documentation</li> <li>• Logs and Inventories</li> <li>• Classification <ul style="list-style-type: none"> <li>➤ Notification</li> </ul> </li> <li>• Retention/Storage</li> <li>• Destruction</li> </ul>

Table 5. Laptop Solutions, Security Certification Exam Training Course. From Ref. [8]

## **APPENDIX E - PROPOSED ISATP MATERIAL OUTLINE**

1. Introduction to Information Assurance
  - 1.1.INFOSEC & COMPUSEC
  - 1.2.Sensitive Data Definition
  - 1.3.Importance of Security
  - 1.4.The Meaning of “Secure”
  - 1.5.Vulnerabilities (and why systems have so many)
  - 1.6.Threats
  - 1.7.Countermeasures
  - 1.8.Policies
  - 1.9.Assurance
2. Network Fundamentals
  - 2.1.Network Types
    - 2.1.1. LANs
    - 2.1.2. WANs
  - 2.2. Network Topologies
    - 2.2.1. Contention-Based (Bus)
    - 2.2.2. Ring
    - 2.2.3. Switched
  - 2.3.Network Devices
    - 2.3.1. Hubs
    - 2.3.2. Switches
    - 2.3.3. Routers
  - 2.4.Important Layer 3/4 Network Protocols
    - 2.4.1. IP
    - 2.4.2. TCP
    - 2.4.3. UDP
    - 2.4.4. ICMP
  - 2.5.How Packets Get Routed
3. Computer System Security and Access Controls
  - 3.1. System Access Control
    - 3.1.1. Identification & Authentication
      - 3.1.1.1. Something you know
      - 3.1.1.2. Something you have
      - 3.1.1.3. Something you are
      - 3.1.1.4. Multiple Factor Authentication

- 3.1.2. Passwords
    - 3.1.2.1. Password Attacks
    - 3.1.2.2. Password Selection
    - 3.1.2.3. Password Protection
  - 3.2. Data Access Controls
    - 3.2.1. Discretionary Access Control
    - 3.2.2. Mandatory Access Control
    - 3.2.3. Access Control List
  - 3.3. Access Control Models
    - 3.3.1. Bell & Lapadula Model
    - 3.3.2. Biba Model
    - 3.3.3. Clark-Wilson Model
    - 3.3.4. Take-Grant Model
- 4. Types Of Attacks
  - 4.1. Probes and Scans
  - 4.2. Account Compromise
  - 4.3. Packet Sniffing
  - 4.4. Denial of Service
  - 4.5. Spoofing
  - 4.6. Malicious Software “Malware”
    - 4.6.1. Viruses
    - 4.6.2. Worms
    - 4.6.3. Trojan Horses
    - 4.6.4. Protecting Against
  - 4.7. Social Engineering
- 5. Intrusion Detection
  - 5.1. Network Based
  - 5.2. Host Based
  - 5.3. Passive Response
  - 5.4. Active Response (IDP)
- 6. Traffic Filtering (Firewalls)
  - 6.1. Types of Firewalls
    - 6.1.1. Stateless
    - 6.1.2. Stateful
    - 6.1.3. Dynamic
    - 6.1.4. Proxy Based
    - 6.1.5. Network Based

- 6.1.6. Host Based (Personal)
  - 6.2. Firewall Configurations
- 7. Cryptography
  - 7.1. Algorithms
    - 7.1.1. Symmetric (Secret Key)
      - 7.1.1.1. DES/3DES
      - 7.1.1.2. AES
    - 7.1.2. Asymmetric (Public Key)
      - 7.1.2.1. RSA
      - 7.1.2.2. Elliptic Curve.
    - 7.1.3. Hashing
  - 7.2. PKI
    - 7.2.1. Digital Certificates
    - 7.2.2. Digital Signatures
    - 7.2.3. PGP
- 8. Steganography
- 9. System Hardening
  - 9.1. Patches
  - 9.2. Principle of Least Privilege Configuration
- 10. Redundancy/Duplication Protection
  - 10.1. Data Backups and Types
    - 10.1.1. Full
    - 10.1.2. Sequential
    - 10.1.3. Differential
  - 10.2. Redundant Systems
- 11. E-mail Security
- 12. Laptop\ PDA Security
- 13. Modem Security

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

1. Commerce Department's Technology Administration, National Institute of Standards and Technology (NIST), Special Pub 800-12, *An Introduction to Computer Security: The NIST Handbook*
2. National Security Telecommunications and Information Systems Security Committee, *National Information Systems Security (INFOSEC) Glossary*, September 2000
3. The Article, *Computer Security Isn't Just Computers*, May 2001
4. SANS Institute Web Site, URL <http://www.sans.org>
5. Naval Postgraduate School Center for INFOSEC Studies and Research (NPS CISR)
6. NPS/CISR Computer Security Course Material, *Introduction to Information Assurance (IA)*, spring 2002
7. Learning Tree International, *Introduction to System and Network Security Course*, January 2003, URL <http://www.learningtree.com/>
8. Laptop Training Solutions, URL <http://www.laptoptraining.com/>
9. Commerce Department's Technology Administration, National Institute of Standards and Technology (NIST), NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, Second Draft, April 2003
10. Kevin Day, *Inside the Security Mind Making the Tough Decisions*, Prentice Hall Inc. 2003
11. Training Requirements for Information Technology Security: *An Introduction To Results-Based Learning*, URL <http://csrc.nist.gov/publications/nistbul/itl98-04.txt>

12. National Security Telecommunications and Information Systems Security Committee, NSTISSI No.4009, June 1992
13. NATO ADatP-2(f), *Automatic Data Processing* (ADP) NATO Glossary, June 1991
14. Brown University, *Information and Data Security Policies*, 1996
15. Microsoft Corporation, *The Definition of a Security Vulnerability*, December 2000
16. Kossakowski, Klaus-Peter. "Glossary of Computer Security Incident Handling Terms and Abbreviations." CERT. 6 March 2000. URL: <http://www.cert.dfn.de/eng/pre99papers/certterm.html>,
17. Alliance for Telecommunications Industry Solutions (ATIS), INFOSEC 99, URL <http://www.atis.org>
18. SearchSecurity.com: The Security-Specific Search Engine, URL <http://searchsecurity.techtarget.com/>
19. Glossary of Telecommunication Terms, 1996 URL <http://www.its.bldrdoc.gov/fs-1037/>
20. Free Online Dictionary of computing FOLDOC, URL <http://foldoc.doc.ic.ac.uk>
21. The School of Computing and Information Technology, URL <http://www.scit.wlv.ac.uk>
22. M-Tech Information Technology Inc., URL <http://m-tech.ab.ca/>
23. Network Security Solutions Ltd, URL <http://www.mynetsec.com/index.htm>
24. Whatis web site part of techtarget network, URL <http://whatis.techtarget.com/>
25. Online dictionary and search engine for computer and Internet technology, URL <http://www.webopedia.com/>
26. John Palumbo, *Social Engineering: What is it, why is so little said about it and what can be done*, June 2000
27. An Introduction to Intrusion Detection Systems and the Dragon IDS Suite, URL <http://www.intrusion-detection-system-group.co.uk/>
28. Microsoft Corp, <http://www.microsoft.com/technet/>

29. Commerce Department's Technology Administration, National Institute of Standards and Technology (NIST), *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST special publication 800-16
30. Entelechy training and performance solutions, URL  
<http://unlockit.com/index.html>
31. Seymour Bosworth, *Computer Security Handbook*, 4th Edition, April 2002

THIS PAGE INTENTIONALLY LEFT BLANK

## BIBLIOGRAPHY

1. Eric Maiwald., *Network Security A Beginner's Guide*, Osborne McGraw-Hill, 2001
2. Charles p. Pfleeger, Shari Lawrence Pfleeger., *Security in computing*, Third Edition, Prentice Hall, 2003
3. A report from a Workshop sponsored by the National Science Foundation and the American association of community colleges, *Protecting Information The Role of Community Colleges in Cybersecurity Education*, Community Colleges Pres, 2002
4. Dorothy E. Denning., *Information Warfare and Security*, Addison Wesley, 2001

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

Defense Technical Information Center

Ft. Belvoir, Virginia

Dudley Knox Library

Naval Postgraduate School

Monterey, CA

Mr. J. D. Fulp

Department of Computer Science

Monterey, CA

Mr. Brian B. Steckler

Graduate School of Operations & Information Sciences

Monterey, CA

Dr. Dan Boger

Chairman, information Warfare Academic Group

Monterey, CA

Captain, Abdulaziz M .Al-Ogail

Dir, Of Technical Support Dept

Riyadh, Saudi Arabia

Rear admiral, Faraj H. Al-Rawdahan

Dir, Of Training Dept

Riyadh, Saudi Arabia

Commodor, Saleh M. Altheneyan

Dir, Information and Computer Dept

Riyadh, Saudi Arabia

Lieutenant, Sami M. Alageel

Naval Postgraduate School

Monterey, CA